ASSESSING THE ALIGNMENT OF INFORMATION SECURITY, STRATEGIC BUSINESS, AND STRATEGIC INFORMATION SYSTEM PLANNING: A DEPARTMENT OF DEFENSE PERSPECTIVE

THESIS

John H. Scanlan IV, Gunnery Sergeant, USMC

AFIT/GIR/ENV/10-J02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/10-J02

ASSESSING THE ALIGNMENT OF INFORMATION SECURITY, STRATEGIC BUSINESS, AND STRATEGIC INFORMATION SYSTEM PLANNING: A DEPARTMENT OF DEFENSE PERSPECTIVE

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

John H. Scanlan IV

Gunnery Sergeant, USMC

June 2010

AFIT/GIR/ENV/10-J02

ASSESSING THE ALIGNMENT OF INFORMATION SECURITY, STRATEGIC BUSINESS, AND STRATEGIC INFORMATION SYSTEM PLANNING: A DEPARTMENT OF DEFENSE PERSPECTIVE

John H. Scanlan IV

Gunnery Sergeant, USMC

Approved:

//SIGNED//	08 June 2010
Dr. Michael R. Grimaila (Chairman)	Date
//SIGNED//	08 June 2010
Mr. Juan Lopez Jr (Member)	Date
//SIGNED//	08 June 2010
Dr. Dennis D. Strouble (Member)	Date

Abstract

This research extends the Strategic Information Systems Plan (SISP) and Strategic Business Plan (SBP) alignment model construct by adding the Information Security Plan (ISP) as an additional component considered essential to the success of network centric organizations. Six hypotheses were considered to measure the two-way alignment among three components of the proposed model. The research was adapted for a public sector organization and analyzed using the Kruskal-Wallis non-parametric test. A vertical, cross-sectional sample from the United States Marine Corps, a Department of Defense organization, was surveyed (n = 149). Results indicate a strong two-way alignment exists between SISP - SBP (p = .232 and .910), between SISP - ISP (p = .445 and .467), and between SBP - ISP (p = .205 and .490). The research instrument developed in this work enables the evaluation of public and private sector organizations determine the strength of their strategic alignment in terms of security, information technology, and business objectives.

Acknowledgments

I would first like to thank my wife for taking care of the kids while I “played on the computer”, “went to school”, or worked through many weekends and holidays. Without your love and support, this would have been much harder than it already was. Thank you Dr. Grimaila for being my advisor and always having positive things to say and answering any question I posed. Juan Lopez, I am truly honored to have worked with you during this experience. Your uncanny wisdom, guidance, and markers were instrumental in keeping me on track… even if it took an hour and a whole 5’ X 10’ dry erase board to answer a simple yes or no question. Working with another Marine made this solo adventure easier.

John H. Scanlan IV

Page

Table of Contents

Page

Page

List of Figures

Page

List of Tables

Page

ASSESSING THE ALIGNMENT OF INFORMATION SECURITY, STRATEGIC BUSINESS, AND STRATEGIC INFORMATION SYSTEM PLANNING: A DEPARTMENT OF DEFENSE PERSPECTIVE

1 Introduction

1.1 Chapter Overview

In this chapter, an overview of the research problem addressed in this thesis is presented. Background information is provided; the problem statement is presented, followed by the research objectives, and hypotheses. The research focus is defined along with motivating factors that contributed towards this thesis. Finally, the assumptions and limitations of this work are presented.

1.2 Background

The private sector continues to adopt Information Technologies (IT) and find innovative ways to leverage it to create competitive advantage. The Department of Defense (DoD) is achieving similar gains to increase combat power capabilities in Network-Centric warfare.

Network-Centric warfare seems to be the latest buzzword for war fighting operations conducted in a man-made virtual domain now formally recognized as Cyberspace. The increased demand for anytime anywhere communications, information sharing, mobility, system interoperability, confidentiality, and distributed operations have resulted in a significant number of asymmetric cyber threats. As a result, network security is considered a key factor to increase mission effectiveness in Network-Centric

Operations (Network Centric Warfare: Report to Congress, Department of Defense 2001). Both the private sector and DoD have demonstrated that a strong alignment between Strategic Business Planning and Strategic Information Systems Planning is a key success factor to achieve competitive advantage and combat power respectively (Network Centric Warfare: Report to Congress, Department of Defense 2001) (Kearns and Lederer 2000).

The Department of Defense (DoD) has been using information technology for many decades to increase productivity and to reduce costs. With the introduction of the Paperwork Reduction Act of 1980 (Public Law No. 96-511. 1980) and the Clinger-Cohen Act (Public Law No.104-106, Division E 1996), indicates the government started to grasp the importance of managing information technology and realized an increase in capabilities (Department of Defense 2006).

Information security has been discussed and well documented for many years within the DoD starting with the Quadrennial Defense Report (QDR) of 2001 (Department of Defense 2001). In the same year the 2001 QDR was released, the report to congress on network centricity was published (Network Centric Warfare: Report to Congress, Department of Defense 2001). The 2006 version of the QDR was focused heavily on cyber warfare. The 2001 Network Centric Warfare Report to Congress highlighted the following statement:

> In a network-centric environment, security is only as good as the weakest link. Since security is essential to warfighting operations, a lack of integrated protection will constrain network-centric applications and/or organizations individually (Network Centric Warfare: Report to Congress, Department of Defense, 2001 pg 6-2).

Security in first sentence of this quote is referencing network/information security and not physical security or another type of security.

Previous research shows an alignment between an information systems plan and the business plan (Kearns and Lederer 2000) (Doherty and Fulford, 2006) (Premkumar and King 1991) (Newkirk and Lederer, 2006) (Burn and Szeto 2000). Other research addresses competitive advantage and how information technology investments are related to information system effectiveness (Chan and Huff 1993) (Kearns and Lederer 2000).

"Network Centric Warfare (NCW) is a warfighting concept that allows us to achieve Joint Vision 2020 operational capabilities" and "…allows the force to achieve an asymmetric information advantage" (Network Centric Warfare: Report to Congress, Department of Defense, 2001 pg. 2-4). Joint Vision 2020 states information superiority is fundamental to the transformation of the operational capabilities of the force (Network Centric Warfare: Report to Congress, Department of Defense, 2001). Information superiority leads to decision superiority, which can be translated into competitive advantage (Network Centric Warfare: Report to Congress, Department of Defense, 2001 pg. 2-6). Information superiority depends on accurate and timely information that is reliable. The security of this information is vital to military success. This translates into Information Assurance providing an uninterrupted flow of authentic communications and information (Network Centric Warfare: Report to Congress, Depatment of Defense, 2004 pg. 3-19).

Information Assurance is often synonymous with Information Security based upon the definition provided in the National Information Assurance Glossary (CNSSI No.

4009, Committee on National Security Systems 2010). These definitions are provided for comparison in Table 1: Definition of IA and IS.

Table 1: Definition of IA and IS (CNSSI No. 4009)

Information Assurance	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security is used in this thesis to encompass the whole umbrella of information protection instead of the measures that protect and defend information.

The importance of Information Security is often under represented and relegated to security experts as an issue to be worked into the business process without affecting functionality. This research proposes to elevate network security on par with Strategic Business Planning and Information Systems Planning. Information security, to include network security, is believed to be an influential factor to achieve combat power (Network Centric Warfare: Report to Congress, Department of Defense 2001).

1.3 Problem Statement

The current literature discussing alignment between Strategic Information Systems Planning (SISP) and Strategic Business Planning (SBP) does not adequately address Information Security (INFOSEC) Planning (ISP). The identification of this gap

in the literature sets the stage for the following question. Does Information Security (INFOSEC) planning fit within the current SISP-SBP alignment model?

This research effort stems from a comment made by a presenter from the office of the Assistant Secretary of Defense/Networks and Information Integration (ASD/NII). This presenter stated the National Security Agencies'' (NSA) Red Team found that the Marine Corps' networks are harder to break into than any other service elements (Grimaila 2009). This research seeks to identify if information security is aligned with the current model.

1.4 Research Objectives

The purpose of this research is to propose INFOSEC as an additional element of the current model construct. An additional purpose of this research is to fill the missing gap in the literature. The current model, depicted in Figure 1, shows the alignment of the Strategic Information Systems Plan (SISP) and the Strategic Business Plan (SPB), which has been studied by numerous authors (Avison, et al. 2004) (Kearns and Lederer 2000) (Motjolopane and Brown 2004) (Powell 1993) (Reich and Banbasat 1996).

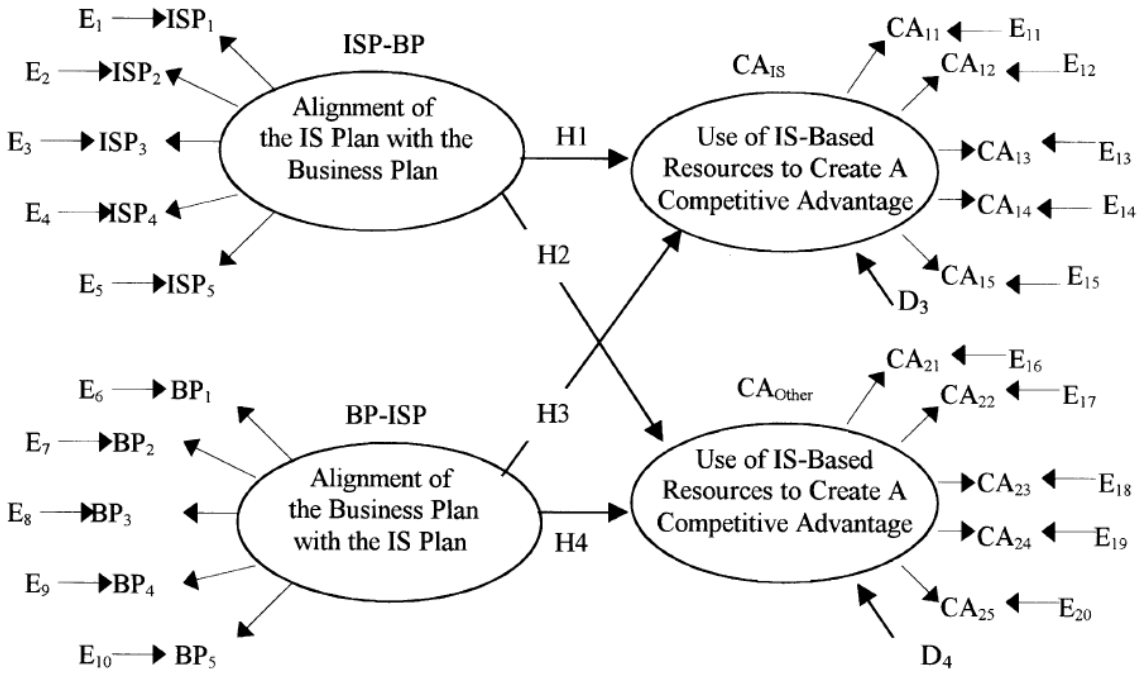

Figure 1: Model of Strategic Alignment (Kearns and Lederer, 2000)

This model appears to be fairly busy; however, the numbering system is quite easy to follow. Each letter represents a particular question the author used in the survey they conducted. The Information Systems Plan (ISP) variable measures the Information System (IS) plan and its alignment with different parts of the organizations business plan (Kearns and Lederer 2000). The variable Business Plan (BP) measures its alignment with the IS plan. The variable Competitive Advantage (CA) measures which IS-based resources are used to create competitive advantage (Kearns and Lederer 2000). The variable E represent elements measuring each hypothesis (5 questions for each hypothesis) and the D variables are disturbance terms for describing the relationship between the constructs (Kearns and Lederer 2000).

The proposed research model is presented in Figure 2: Proposed Model. The proposed research model introduces the additional element of Information Security to the current model with the goal of assessing the alignment between the Strategic Information Systems Plan (SISP) and the Strategic Business Plan (SBP).

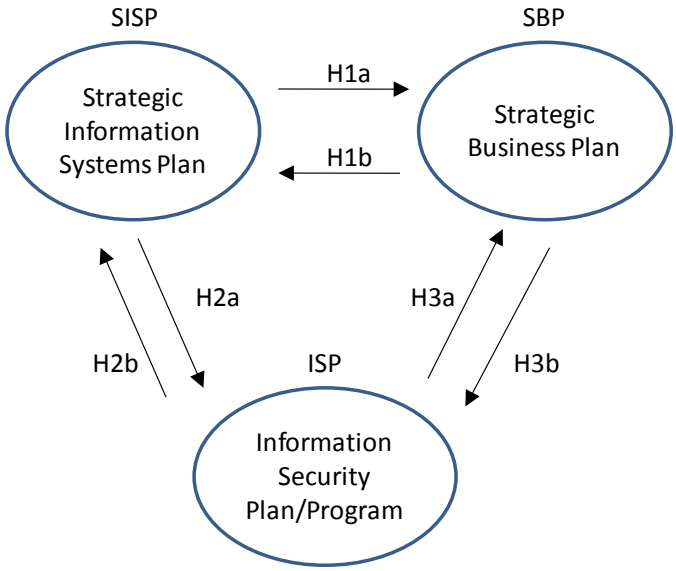

Figure 2: Proposed Model

A motivating factor for this research stems from the comment stated earlier that *"Marine Corps' networks are harder to break into."* This research is motivated by the need to understand some aspect of "why". Every service component implements network defense commits resources and personnel to maintain a security capability. This research looks beyond the technical aspects of information security and focuses on the perceptions of the people, (i.e. Technicians, Middle Managers, and Senior Managers). Often overlooked are the lower level operators and people who implement or follow orders. How do the operators, supervisors, mangers, and senior leadership feel about the

alignment of information security or information assurance within the United States Marine Corps?

1.5 Hypotheses

The first two hypotheses are derived from a survey conducted by Kearns and Lederer titled "The effect of strategic alignment on the use of IS-based resources for competitive advantage" (Kearns and Lederer 2000). The referenced study attempted to define the alignment dichotomy of the strategic business plan and the strategic information systems plan. Although one of the main tenants of the previous study was competitive advantage, the alignment questions that were presented to show alignment were adopted for this study with minor changes to suit the environment. Competitive advantage in the Kearns and Lederer study refers to the competencies, capabilities, and resources that provide a distinct attraction to customers and create superiority over competitors (Kearns and Lederer 2000). Competitive advantage was chosen as a construct because organizational performance has been linked favorably to it in the literature. Due to the nature of the military as a not-for-profit organization, competitive advantage takes on a different form as compared to a for-profit business. Competitive advantage for the Department of Defense (DoD) could include such things as increased situational awareness, real-time command and control (C2), and advanced information sharing in an increasingly net-centric world.

The hypotheses presented in this research are listed in Table 2: Research Hypotheses Each hypothesis contains five questions assigned to measure alignment.

Three mutually exclusive groups will be measured for the six hypotheses. The groups are categorized as Technicians, Middle Managers, and Senior Managers.

Table 2: Research Hypotheses

Hypothesis 1a:	There is alignment between the Strategic Information System Plan (SISP) and the Strategic Business Plan (SBP).
Hypothesis 1b:	There is alignment between the Strategic Business Plan (SBP) and the Strategic Information System Plan (SISP).
Hypothesis 2a:	There is alignment between the Strategic Information System Plan (SISP) and the Information Security Plan (ISP).
Hypothesis 2b:	There is alignment between the Information Security Plan (ISP) and the Strategic Information Systems Plan (SISP).
Hypothesis 3a:	There is alignment between the Information Security Plan (ISP) and the Strategic Business Plan (SBP).
Hypothesis 3b:	There is alignment between the Strategic Business Plan (SBP) and the Information Security Plan (ISP).

1.6 Research Focus

The primary research focus for this study is information security professionals within the Department of Defense, specifically the United States Marine Corps. A stratified sample of information security professionals within the Marine Corps was

sampled. This stratification should be representative of the Department of Defense population of information security professionals.

1.7 Assumptions/Limitations

There are five main assumptions made in this study. First, that survey respondents have adequate experience to answer questions pertaining to the alignment of security policies and operational planning. Second, the intended sample can understand the questions being asked in the survey instrument. Third, the server hosting the online survey at the Air Force Institute of Technology will function as required, be available to display the survey, and record responses from the survey takers. Fourth, the response rate should be sufficient to infer results about the intended research questions. Finally, the sample population is mutually exclusive.

A limiting factor for gathering responses is the operational tempo and deployment status of the information security professionals within the Marine Corps. Another limiting factor and assumption is the research method used to collect responses for the survey.

1.8 Implications

This research introduces Information Security (INFOSEC) to the existing alignment model construct between Strategic Information System Planning (SISP) and Strategic Business Planning (SBP). The research approach sampled a vertical cross section of the Information Assurance (IA) workforce unlike similar studies which surveyed upper management and executive level personnel. The results indicate how

three independent groups (Technicians, Middle Management, and Senior Management) perceive alignment. In conjunction with measured security capabilities, the alignment measurements may be used to predict security capabilities with other organizations. The results of the study should be replicated with other military, public and private organizations to see if information security alignment is a valid component of the proposed model construct.

1.9 Summary

This first chapter discussed the background for this thesis. The problem statement is outlined along with the research objectives. The research questions are listed and the research focus is discussed. Assumptions and limitations are presented in addition to the implications of this study. The next chapter contains literature review and presents the background information in more detail.

2 Literature Review

2.1 Chapter Overview

This chapter contains background information as well as review of the literature. The topics discussed in this chapter are the Strategic Information System Plan (SISP), the Strategic Business Plan (SBP), and an introduction of Information Security Plan (ISP). The roles and responsibilities of the corporate level personnel are briefly discussed.

2.2 Relevant Research

2.2.1 Strategic Information Systems Plan

The literature review on Strategic Information Systems Plan (SISP) has grown considerably since it was conceptually introduced by (Lederer and Sethi, 1988). The Strategic Information Systems Plan was based upon early research concerning Management Information Systems in the late 1970's (King, 1978).

2.2.2 Strategic Information Systems Planning

The most recognized definition of Strategic Information Systems Planning is "the process of identifying a portfolio of computer-based applications that will assist an organization in executing its business plans and realizing its business goals (Lederer and Sethi, 1988 pg. 446).

The Strategic Information Systems Plan is a result of the Strategic Information Systems Planning process. The planning process for SISP has drawn the attention of academia for several years. Strategic information planning gives managers the opportunity to indentify broad initiatives, specific applications, and critical technologies

to help their organizations carry out their current business strategy more successfully (Lederer and Gardiner, 1992).

Strategic information systems' planning has been studied intensely over the past few decades. The most common definition referenced for strategic information systems planning emanates from research by Lederer and Sethi: "the process of identifying a portfolio of computer-based applications to help an organization achieve its business goals" (Lederer and Sethi, 1988) (Newkirk, Lederer, and Johnson, 2008) (Lederer and Salmela, 1996) (Hevner and Studnicki 2000) (Lederer and Gardiner, 1992) (Philip 2007) (Brown, 2008).

Due to environmental conditions and uncertainty inherently involved in planning, the most appropriate view of strategic information systems planning is derived from the initial theory of strategic information systems planning (Lederer and Salmela, 1996). The theory presented is based upon earlier research where information systems' planning is described as "a system comprised of inputs, processing, and outputs (King, 1988). "The theory of information systems planning states the result of information systems planning is an information plan whose major component is a set of recommendations for new information systems" (King, 1988). The theory of information systems planning has seven constructs: (1) the external environment, (2) the internal environment, (3) planning resources, (4) the planning process, (5) the information plan, (6) the implementation, and (7) the alignment of the information plan with the organization's business plan (Lederer and Salmela, 1996). The theory is graphically represented in Figure 3 and shows the constructs of the theory with alignment arrows.

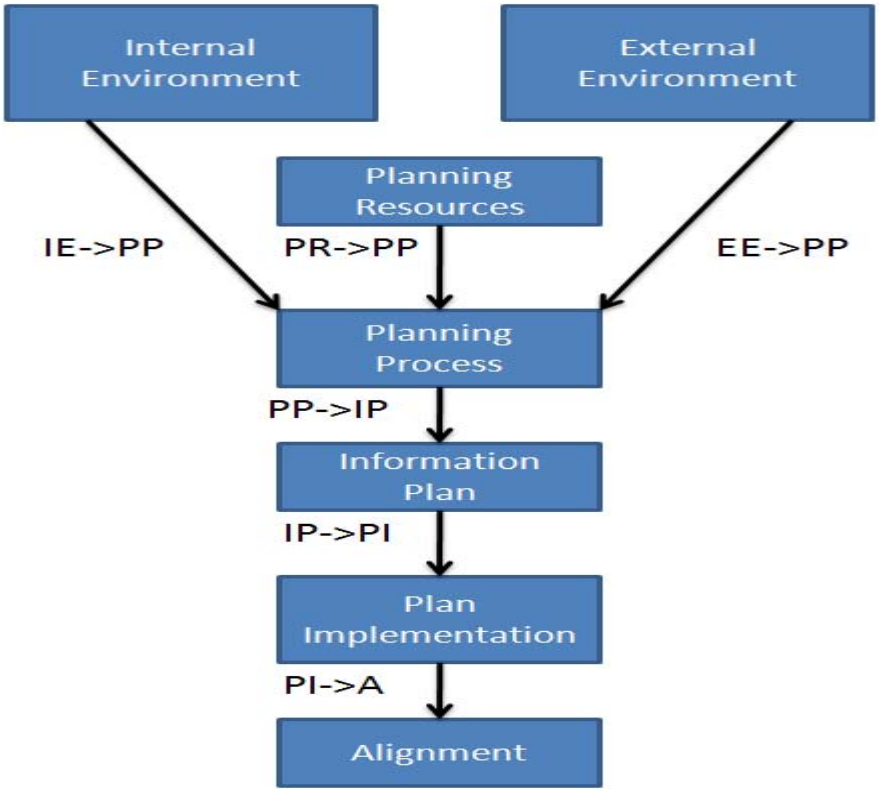

Figure 3: Theory of Information Systems Planning (Lederer and Salmela, 1996)

The internal environment contains several variables including an organizations size, information systems planning style, culture, planning goals, and objectives (Lederer and Salmela, 1996). An organizations' size can influence information systems planning because larger organizations tend to have a more formal planning process and are usually more experienced at information systems planning (Lederer and Salmela, 1996). Culture also can have an effect on information systems planning. In the military, specifically the U.S. Marine Corps, planning is an essential and significant part of command and control (Marine Corps Doctrinal Publication 5 1997).

The external environment is an area outside the control of the organization and includes all variables that can affect the planning process. Some external variables

include changes in supplier trends, customer preferences, government legislation, and competitors' actions that can influence the information systems planning process (Lederer and Salmela, 1996).

Planning resources is an important stage in information systems planning theory and includes planners, other professionals, and software in addition to traditional resources involved in the planning process. Additionally, the organizations business plan can be seen as an important planning resource. Many strategic information systems planners adhere closely to the business plan as they develop the information plan (Lederer and Salmela, 1996).

The typical strategic information systems planning process requires following a series of well-defined steps (Lederer and Salmela, 1996). Depending on organizational needs this planning process can be exhaustive and time consuming or short and simple. According to Flynn and Goleniewska (1993), several planning methodologies have been studied and analyzed including the Ward et.al approach, Information Engineering, the Dickerson and Wetherbe approach, the multidimensional approach, Information Strategy Planning (ISP)), and the Andersen Consulting referenced as Method/1 (Lederer and Salmela, 1996).

The contents of the information plan depend on the process and methodology used in the planning process. Organizations typically leverage meetings, interviews, and document analysis in the planning process. Smaller organizations typically do not have sufficient resources or the manpower available to produce a robust information plan. A

planning process of higher quality produces an information plan of greater quality (Premkumar and King 1991).

The output of the strategic information systems planning process results in the information plan (Lederer and Salmela, 1996). Implementing the information plan is an important construct of information systems planning. Organizations often fail to properly implement the information system plan which is recognized as a serious problem (Lederer and Sethi, 1988) (Lederer and Salmela, 1996). However, clear goals, formal planning, and organizational resources are key to successful implementation (Premkumar and King 1991).

2.2.3 Strategic Planning Process

According to Powell (1993), the purpose of information systems – and thus the purpose of strategic information systems planning for them – is to effect the organization favorably. The term fit has been coined as the alignment between the information plan and the business' goals and objectives (King, 1978). King defines alignment as "the degree to which the information systems plan reflects the business plan". A measure to assess alignment of the information systems plan is the fulfillment level of defined goals and objectives within the information systems plan (Premkumar and King 1991) (Raghunathan and Raghunathan 1994).

The strategic planning process has five phases with specific tasks within each phase (Mentzas, 1997). The research conducted by Newkirk and Lederer (2007) describes the phases in more detail.

2.2.3.1 Phase 1

The first phase is called strategic awareness. In the first phase, all key issues are identified along with planning objectives. The first phase also organizes planning teams and ensures top management is involved.

2.2.3.2 Phase 2

The second phase is situation awareness. During the second phase, the current business systems are analyzed along with other important business systems used to support organizational operations. External systems are also examined to determine business impact and can be improved.

2.2.3.3 Phase 3

The third phase is referred to as strategy conception. During the third phase, the IT objectives are identified. Improvement opportunities and IT strategies are documented.

2.2.3.4 Phase 4

The fourth phase, called strategy formulation, consists of identifying the business process, IT architectures, and any IT projects.

2.2.3.5 Phase 5

The fifth phase, strategy implementation, provides a detailed plan of action that supports the implementation strategy.

Successful SISP implementation depends on whether or not the objectives mentioned in the plan are achieved (Raghunathan and Raghunathan, 1994). SISP success has also been linked objectives such as alignment, analysis, cooperation, and improvement in capabilities (Segars and Grover, 1998).

2.2.4 Strategic Business Plan

A strategic business plan is a roadmap for the organization and details the business operation. In terms of strategic planning, the business plan has also been referred to as an organizational strategy set, which consists of the business mission, objectives, strategy, and other strategic organizational attributes (King, 1978). An organization's mission, usually in the form of a mission statement, describes what the business does, why it exists, and what contributions the business can make, and describes the business objectives (King, 1978).

According to Croteau and Bergeron, business strategy is defined as actions taken by an organization to reach its objective. Furthermore, they describe strategy as an outcome of decisions made to guide an organization with respect to the environment, structure and processes that influence its organizational performance (Croteau and Bergeron, 2001).

2.2.5 Strategic Alignment

Alignment has been defined as the degree to which the IT mission, objectives, and plans support and are supported by the business mission, objectives, and plans (Reich and Banbasat, 1996). While this definition has been used as the definition for much of the research centered on strategic alignment the fundamental definition comes from earlier research (Kearns and Lederer, 2000) (Lindstrom, Samuelsson, Harnesk, and Hagerfors, 2000).

Early research denotes that there is an intrinsic linkage of the decision supporting MIS to the organization's purpose, objectives, and strategy (King, 1978). In the late

1970's, King noted there was a lack of literature regarding the alignment between management information systems (MIS) and the business plan. King noted that MIS was being developed strategically however, much of the focus was on the systems themselves and that a bottom-up approach was being used to plan strategically. The need for strategic information systems planning and integration with the business plan had not been developed. King's contribution was the realization of the relationship between the strategic information systems plan and business planning objectives, which has been cited often since its inception (Teo and King, 1997) (Henderson and Venkatraman, 1993) (Newkirk and Lederer, 2007) (Doherty, Marples, and Suhaimi, 1999) (Newkirk, Lederer, and Johnson, 2008)

Building on King's work in 1978, Henderson and Venkatraman developed a strategic alignment model to show alignment between IT strategy and business strategy. The strategic alignment model is founded on two main principles: strategic fit and functional alignment (Henderson and Venkatraman, 1993).

Figure 4 is broken up into four main domains: Business strategy, I/T strategy, Organizational Infrastructure and Processes, and I/S Infrastructure and Processes (Henderson and Venkatraman, 1993). Vertically referencing the model, there are two columns that split the model into business and information technology. On the left, the business side, there is business strategy and organizational infrastructure and processes. On the right, which is the I/T side, there is I/T strategy and I/S infrastructure and processes. Horizontally referencing the model along the first row, there is the external domain made up of business strategy and I/T strategy. Along the second row of the

model, the internal domain consists of organizational infrastructure and processes and I/S infrastructure and processes.

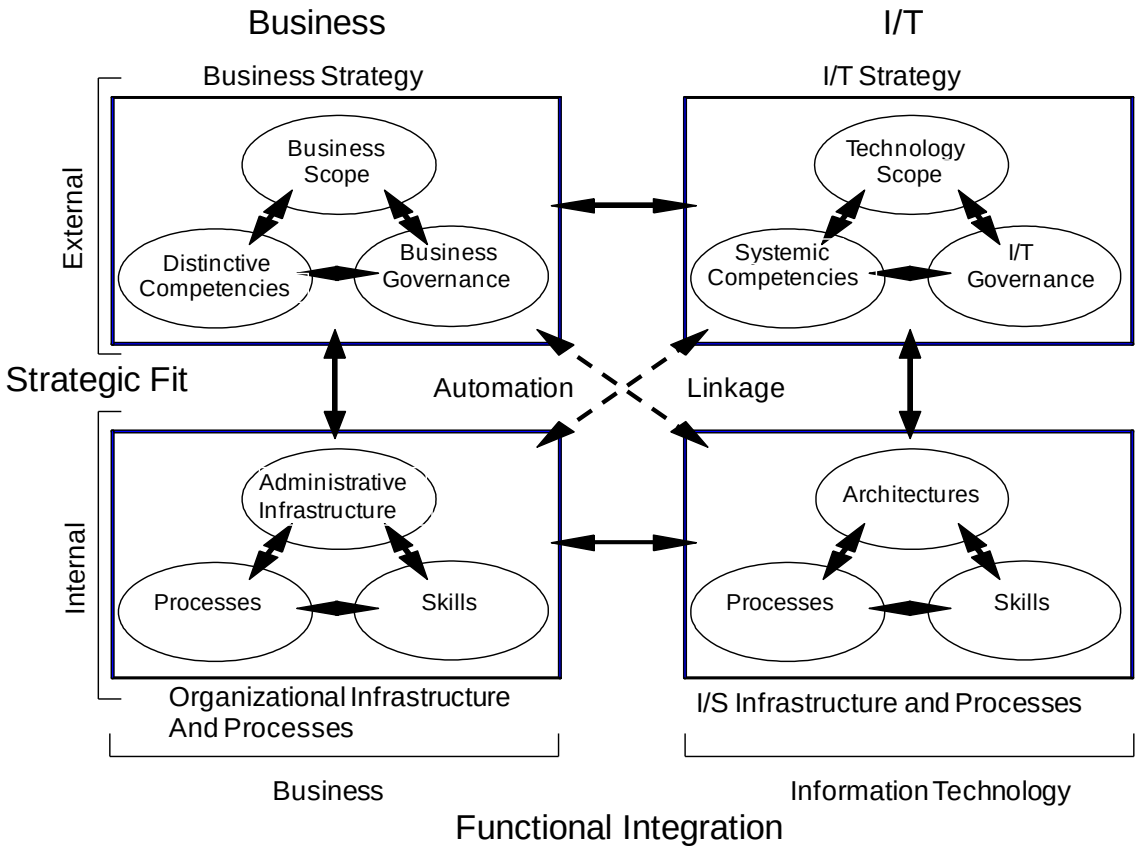

Figure 4: Strategic Alignment Model (Henderson and Venkatraman, 1993)

This figure is an adaptation of a Microsoft PowerPoint presentation developed for the Tampa Bay Technology Leadership Association (Papp and Lackey 2007) (Tampa 2010).

The alignment between the external and internal domains is called Strategic Fit. Strategic fit, also referenced as strategic integration, is the alignment between the business strategy and the I/T Strategy that enables the capability of IT to shape and support the business strategy (Henderson and Venkatraman, 1993). The linkage between

the internal domains is called functional integration because this is where the business processes and IT processes come together to form the business operational capabilities.

A premise of the strategic alignment model is that effective IT management would require a balance of choices across all of the domains. One way to accomplish these choices is to look at bivariate relationships between the domains which are described as perspectives (Henderson and Venkatraman, 1993).

The first perspective shown in Figure 5 is called strategy execution. This perspective is grounded in business strategy. Business strategy is the driver for organizational design choices and the design of the I/S infrastructure. This perspective could be viewed as the most widely accepted view because it corresponds to the hierarchical view of strategic management (Henderson and Venkatraman, 1993).

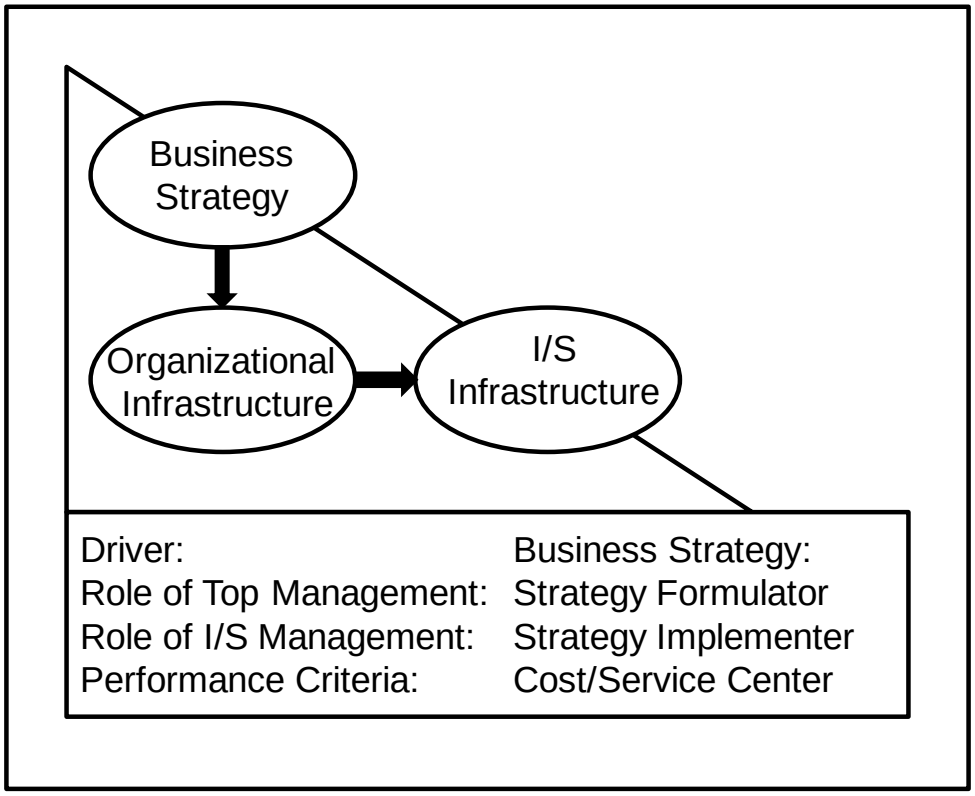

Figure 5: Strategy execution alignment (Henderson and Venkatraman, 1993)

The second perspective in the strategic alignment model, shown in Figure 6 is called technology transformation. Unlike the first perspective where the business strategy is implemented through the organizational infrastructure to influence the I/S design choices, this perspective uses the I/T strategy to implement the business strategy. The role of top management is to provide the business strategy for I/S management to implement.

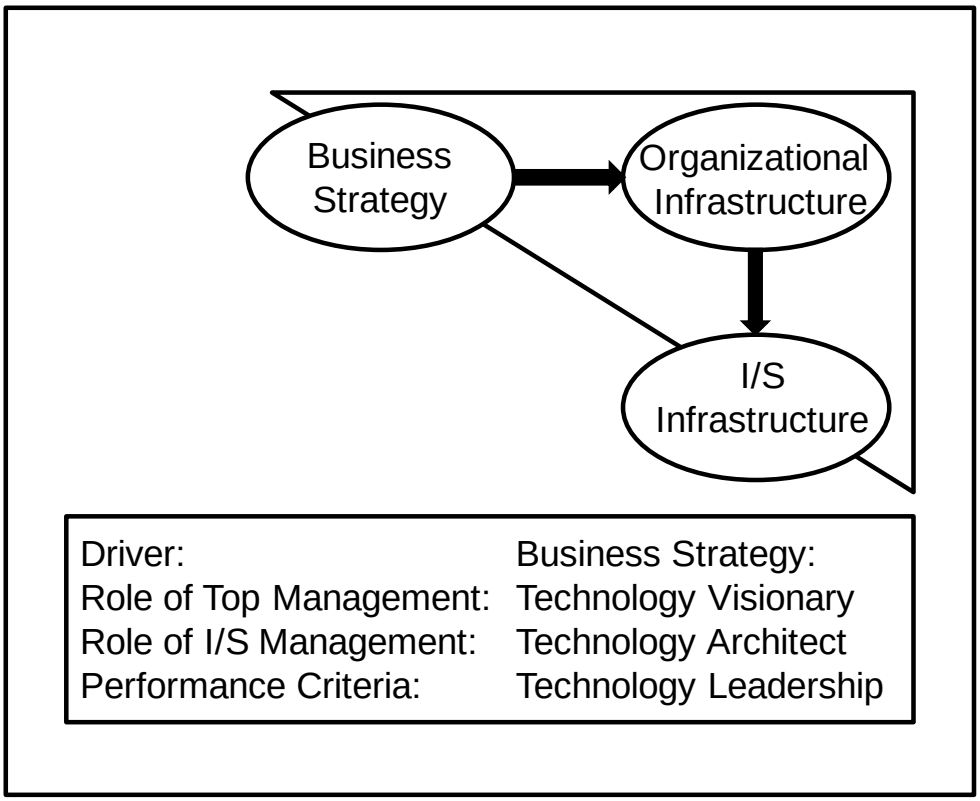

Figure 6: Technology transformation alignment (Henderson and Venkatraman, 1993)

Using this view of the strategic alignment model allows businesses to embrace the latest technology through the I/T strategy to build the I/S infrastructure to support the business objectives. The technology transformation alignment perspective allows managers to forecast technology and build the I/S infrastructure to suit the needs of the business. The role of top management in this perspective is to provide a vision for technology that I/S managers can use.

The third perspective is called competitive potential alignment. The premise behind competitive potential shown in Figure 7 is businesses seek out emerging

technological capabilities that align with the business strategy to improve the organization.

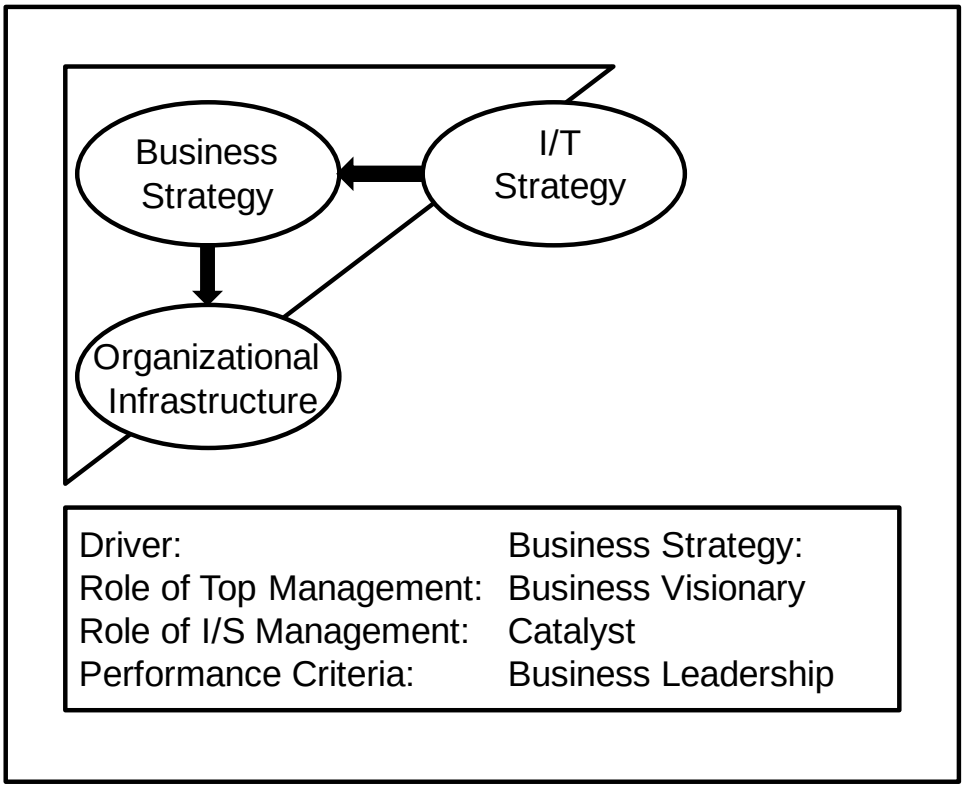

Figure 7: Competitive potential alignment (Henderson and Venkatraman, 1993)

The I/T strategy lends itself to changing the business strategy according to changing technology. This in turn forces the business strategy down to the organization for adaptation. The role of top management here is business vision. If top-level managers have I/S managers that are tech savvy, they can update the managers on new technology, which will allow management to capitalize on emerging technologies and then merge them with the business strategy. The I/S manager is viewed as the catalyst for this technology integration into the business plan by aligning the I/S strategy with the business strategy.

The final perspective in Figure 8 is referred to as the service level alignment perspective.

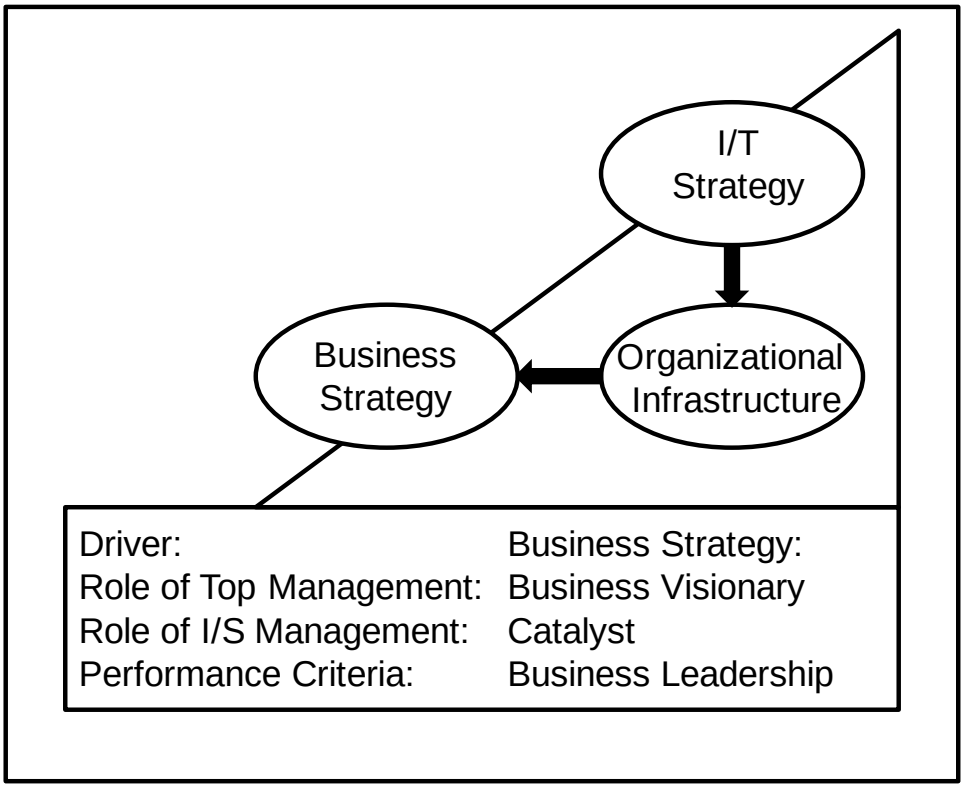

Figure 8: Service level alignment (Henderson and Venkatraman, 1993)

Henderson and Venkatraman (1993) describe the alignment perspective that focuses on how to build a world-class I/S service organization. This alignment allows the I/T strategy to influence the I/S infrastructure which drives the organizational infrastructure. The role of business strategy is viewed as providing direction but is not the focus. The role of top management in this perspective is to prioritize the use of resources. Top management allocates the resources to be used within the business environment. The I/S manager is viewed as the executive leader that will make most of the I/S decisions affecting the organization.

The strategic alignment model discussed is only the foundation for viewing strategic alignment. There have been a few researchers who have analyzed the strategic alignment model (Avison, Jones, Powell, and Wilson, 2004) (Baets, 1992). Table 3 shows a brief representation of authors who have referenced the strategic alignment model by Henderson and Venkatraman over the past ten or more years. This list of references is by no means all inclusive or exhaustive. This table is meant to show these are a few authors who have referenced the strategic alignment model in their publications.

Table 3: Authors who have referenced Strategic Alignment Model

Authors	Year											
	96	97	98	99	00	01	02	03	04	05	06	07
Avison et. al.									X			
Doherty, N. F., Marples, C. G., & Suhaimi, A.				X								
Hevner, A. R., & Studnicki, J.					X							
Kearns, G. S., & Lederer, A. L.					X							
Mentzas, G.		X										
Motjolopane, I., & Brown, I.									X			
Newkirk, H. E., & Lederer, A. L.												X
Peppard, J., & Ward, J.									X			
Reich, B. H., & Benbasat, I.	X				X							
Sabherwal, R., & Chan, Y. E.						X						
Segars, A. H., & Grover, V.			X									
Teunber, R. A.												X

Although there are many references to the strategic alignment model, much of the focus in the literature has been on the alignment of the strategic information systems plan to the business plan and the planning process.

Table 4: Authors who reference Strategic Planning or Strategic Alignment (or both)

Authors	Year																			
	78	87	88	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08
Avison et. al.																X				
Beats, W.				X																
Brown, I.															X					X
Chan, Y. E., & Huff, S. L.					X															
Coleman, P., Papp, R.																		X		
Doherty, N. F., Marples, C. G., & Suhaimi, A.											X									
Flynn, D. J., & Goleniewska, E.					X															
Gottschalk, P.											X									
Hartono, E., Lederer, A. L., Sethi, V., & Zhuang, Y.															X					
Hevner, A. R., & Studnicki, J.												XX								
Kearns, G. S., & Lederer, A. L.												X								
King, W. R.	X																			
Lederer, A. L., & Gardiner, V.				X																
Lederer, A. L., & Sethi, V.			X																	
Masa'deh, R., Hunaiti, Z., Yaseen, A																				X
Mentzas, G.									X											
Motjolopane, I., & Brown, I.																X				
Newkirk, H. E., & Lederer, A. L.																			X	
Peppard, J., & Ward, J.																X				
Philip, G.																			X	
Pollalis, Y. A.															X					
Powell, P.					X															
Raghunathan, B., & Raghunathan, T. S.						X														
Reich, B. H., & Benbasat, I.								XX				X								
Rogerson, S., Fidler, C.						X														
Sabherwal, R., & Chan, Y. E.													X							
Segars, A. H., & Grover, V.										X										
Teo, T. S., & King, W. R.									X											
Teunber, R. A.																			X	
Venkatraman, N., & Ramanujam, V.		X																		
Yarberry, W. A.																	X			

As shown in Table 4, thirty-three authors over the past thirty years have researched or referenced the strategic planning process or have focused on the alignment between the strategic information systems plan and how it relates to the business plan. The representation in Table 4 is not a total representation of all of the authors who have

written or researched the strategic information systems planning process or the alignment between the strategic information systems plan and the business plan. Some authors, such as Reich, B.H., and Benbasat, I, and Hevner, A.R., and Studniki, J., have published several articles about the subject in either the same year or a subsequent year. In this case, two XX's were used to annotate this in the table.

2.2.6 Indicators of Strategic Alignment

Strategic IS alignment is the linkage of the firm's IS and business plans (Premkumar and King 1991). Indicators range widely from completion of projects to operating within a budget (Gottschalk 1999). An indication of alignment is the presence of a written plan consisting of IT projects that assist a business in realizing their goals (Gottschalk 1999). Gottschalk (1999) also pointed out that responsibility and user involvement are the two most important indicators of alignment. Responsibility refers to senior management taking responsibility for IT/IS plan implementation instead of participating only in the strategic planning process. User involvement refers to the user being involved during implementation of an IT/IS plan.

The process of planning an implementation of the SISP is a predictor of strategic alignment (Hartono, et al. 2003). Previous authors also identified the importance of management involvement in the planning process and team member selection as important factors of strategic information systems planning (Hartono, et al. 2003).

2.2.7 Information Security Plan

An information security policy is defined as 'a broad guiding statement of goals to be achieved' with regard to security of corporate information resources (Doherty and

Fulford, 2006) (ISO/IEC 17799, 2005). Both public and private sectors of business have information security policies and programs in place. The breadth of these policies and programs vary greatly. The application and comprehensiveness of security plans and policies was not within the scope of this research and were therefore not investigated further.

The main focus of this research effort is to present the aspect of aligning information security with the strategic information systems plan as well as with the strategic business plan. The need for aligning information security with information systems planning has been previously considered (Lindstrom, et al. 2000) (Doherty and Fulford, 2006).

> "Alignment is about achieving synergy between strategy, organization, process, technology, and people in order to sustain the quality of interdependence and thus achieve competitive advantage" (Lindstrom, et al. 2000).

The area of strategic planning for information security is still immature and needs further development. Information Security is considered along with the culture of the organization, the business requirements, and people when deciding on which security controls and security standards will be incorporated into the business strategy and SISP. Alignment between strategic planning of information systems and security policies is often missing or not adequately addressed by senior management. (Lindstrom, et al. 2000).

2.2.8 Who is in charge?

As with any organization, a company is only as strong as its people. A company can also be viewed as being strong if they have strong leadership and a proven success record (Duffy 2006). The key decision markers in corporate level business usually have 'Chief' or Executive in their title. Such titles include but are not limited to; Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Operations Officer (COO), Chief Information Officer (CIO), and Executive Vice President (EVP) to name a few (Occupational Information Network 2010). The most common tasks chief executives perform are referenced in Table 5 below.

Table 5: Chief Executive Tasks (O*NET), 2010

• Direct and coordinate an organization's financial and budget activities to fund operations, maximize investments, and increase efficiency. • Confer with board members, organization officials, and staff members to discuss issues, coordinate activities, and resolve problems. • Analyze operations to evaluate performance of a company and its staff in meeting objectives, and to determine areas of potential cost reduction, program improvement, or policy change. • Direct, plan, and implement policies, objectives, and activities of organizations or businesses to ensure continuing operations, to maximize returns on investments, and to increase productivity. • Prepare budgets for approval, including those for funding and implementation of programs.	• Direct and coordinate activities of businesses or departments concerned with production, pricing, sales, or distribution of products. • Negotiate or approve contracts and agreements with suppliers, distributors, federal and state agencies, and other organizational entities. • Review reports submitted by staff members to recommend approval or to suggest changes. • Appoint department heads or managers and assign or delegate responsibilities to them. • Direct human resources activities, including the approval of human resource plans and activities, the selection of directors and other high-level staff, and establishment and organization of major departments.

Within the DoD, these tasks usually do not fall within the responsibility of one person. Typically a commissioned military officer, will assume many of the tasks as they progress in their career. To compare executive level positions to military positions is not an easy task. The higher a person's rank, the more executive level tasks they assume. Most of the current CEO's with military experience left the military as either Lieutenants or Captains (Duffy 2006). Most of the CEO grooming occurs within the first ten years of a military career for officers compared to enlisted personnel.

2.3 Summary

This chapter discussed the background information concerning the Strategic Information Systems Plan (SISP), the Strategic Business Plan (SBP), and the Information Security Plan (ISP). Strategic alignment was also detailed to give the reader a better insight of how alignment is perceived. The chapter closes with giving a snapshot of the roles and responsibilities of the people who are in charge of an organization. The next chapter will lay the framework of this research and the methodology.

3 Methodology

3.1 Chapter Overview

This research uses a quantitative approach through the application of directional hypothesis testing as the study methodology. Predictions about relationships among three groups from the information security discipline are tested empirically. The primary data collection tool is a survey instrument. Supporting detail describing the research approval process, survey design, pilot survey, data collection method, target population characteristics, sample size determination, expected response rates, and statistical analysis technique are also presented.

3.2 Research Approval

Approval to conduct research with US Air Force human subjects requires strict adherence to Air Force Instruction (AFI) 36-2601. Additionally, the survey instrument and research methodology must be approved by the AFIT institutional review board to ensure the safety and protection of human subjects and the data collected from them. Occasionally, the research can qualify for exemption based on predetermined research activity involving survey instruments or methods. The investigator must contact the local IRB prior to initiating a research. The IRB will determine if the research (1) is exempt from further review or (2) the study presents minimal risk and is eligible for expedited review; or if (3) the study requires full board review (AFI 40-402). . When sampling non-Air Force personnel an exemption can be requested to defer to the judgment of a locally assembled Institutional Review Board vice requiring an external approval to

conduct the research (AFI 40-402). An exemption was requested and granted on December 17, 2009 and is provided in Appendix A.

3.3 Population

The target population for this study is the Department of Defense (DoD) Information Assurance (IA) Workforce. The IA workforce consists of personnel performing IA functions to establish IA policies and implement security measures and procedures for the Department of Defense and affiliated information systems and networks (DoD 8570.1-M). The heads of each DoD component have the responsibility to develop their IA workforce in accordance with the DoD IA workforce improvement program. Although the military establishment typically equates responsibilities along a linear rank progression structure, the IA workforce categories or specialties and levels do not necessarily correlate to civilian grades, military ranks, or any specific occupational classification standard. For this reason, the demographic portion of the survey instrument was designed to account for this disparity. This allows for categorizing each respondent into a mutually exclusive group. The population includes all ranks within the enlisted community and Colonel and below within the officer community. Also included are civilians, contractors, and government employees.

3.4 Representative Sample

The US Marine Corps IA workforce is representative of the target population and was selected for sampling. The Information Assurance Division at Headquarters U.S. Marine Corps Command, Control, Communications, and Computers (HQMC C4)

maintains a listing of the USMC IA workforce. The population information was obtained on 26 March 2010 and was the baseline used for this study.

The sampling strategy used for this study is a proportional stratified random sample. Due to military workforce shaping (known as grade shaping) provides a pyramid shaped workforce. Large quantities of entry level personnel are near the bottom of the pyramid while fewer numbers of more senior personnel are located near the top of the pyramid. Due to grade shaping effects and the resulting unequal size of each stratum, a more appropriate approach is to use a random sample proportional to each stratum identified in the USMC IA workforce. The approach has the advantage of guaranteeing equal representation of each of the identified strata.

The Information Assurance Division (IAD) at Marine Corps Command, Control, Communications, and Computers (C4) hosts a Microsoft Excel™ spreadsheet, called the "IA Contacts list", which lists Information Assurance professionals throughout the Marine Corps by rank, last name, first name, billet/position, phone number, and email address. Having access to this resource makes stratified random sampling advantageous to obtaining results from the information assurance community. Excluded from this study are Marines in a reserve capacity. The list of names maintained at Marine Corps Command, Control, Communications, and Computers (C4) contain only active duty Marines, government employees, contractors, and civilians working in an information assurance billet. The decision was made by the author to exclude E1 to E4 and GS 5 and below because personnel at this rank usually do not have adequate experience to answer questions relating to military planning and alignment between higher-level policies.

3.5 Sample Size

The sampling strategy used for this study is stratified random sampling. Determining the sample size is a common goal of research to ensure representativeness of the population (Bartlett, Kotrlik and Higgins 2001). The population for this survey is n=344. The population size is derived from the IA Contacts list provided by Marine Corps Command, Control, Communications, Computers (C4) and hosted on their website. Since the information obtained is For Official Use Only (FOUO), reference to this file and site would be inappropriate in this study.

The margin of error is an estimate of the level of risk the researcher is willing to accept. The alpha level is the level of risk the researcher is willing to accept that the true margin of error exceeds the acceptable margin of error (Bartlett, Kotrlik and Higgins 2001). The alpha level used in determining sample sizes in most educational research is either .05 or .01 (Bartlett, Kotrlik and Higgins 2001). Commonly referenced is Cochran's formula for estimating sample size where the t-value for alpha level .05 (α = .05) is 1.96 for sample sizes above 120 (Cochran 1977). Krejcie and Morgan maintain that for continuous data, a 3% margin of error is acceptable (Krejcie and Morgan 1970). Using a five point likert scale, 3% margin of error of the true mean would be calculated as .03 times five (.03 * 5 = .15). Therefore, the sample responses should be with of the mean.

Variance estimation for a five point likert scale is calculated as 1.25. Where S = . Where 5 = number of points in the likert scale and 4 = number of standard deviations.

The formula the researcher used for determining an acceptable sample size is:

Figure 9: Formula for Acceptable Sample Size (Bartlett, Kotrlik and Higgins 2001)

This sample size is also in line with the recommended guidelines presented by (Gay 2005) which state the following:

- For populations (N<100), survey the entire population.
- For populations (N= 500), 50% of population should be sampled.
- For populations (N= 1500), 20% of population should be sampled.
- For populations (N>5000), sample size should = 400.

Given the population size of 344, and the availability of nearly 100 percent of the populations' email addresses, the whole population will be given access to the survey by way of email directing respondents to a specific website hosted by the Air Force Institute of Technology. In an attempt to elicit a better response rate, the survey solicitation email was sent from the office of the senior Marine Corp Information Assurance Chief.

The survey was made available to the information assurance community during the 10th annual Information Assurance conference held in Palm Desert, California during the last week of March 2010. The survey responses collected during the conference are combined with the overall survey responses because they are stored within the same database on the hosting web server.

3.6 Response Rate

An average response rate from a web survey is 32.52% based upon a meta-analysis of 199 surveys (Hamilton 2009). Given the population of 344, the expected response rate should be 112 or greater (= .325581 or 32.56%). This average response rate was the average of all of the surveys conducted in the overall meta-analysis. The average response rate with a sample size less than 1000 is 41.21% (Hamilton 2009). With the population of 344, in order to obtain a response rate of 41% there need to be at least 142 valid responses (= .412790 or 41.28%).

3.7 Pilot survey

A pilot survey was conducted and distributed to mainly the Cyber Operations students of the Air Force Institute of Technology and a few Marine students who were enrolled in an environmental program. The students provided grammatical corrections and grammar suggestions to the survey questions. Most of the students indicated they had no practical knowledge to answer the questions on the survey. Since the survey is designed for the Marine Corps information assurance community, the Marine students who did respond were either aviators or engineers and could not provide adequate answers to the questions.

3.8 Survey Assumptions

The following assumptions are made for the survey:

1. Each respondent will only complete one survey and not submit multiple surveys.

2. Each respondent will choose the correct combination of Rank, MOS, and Years of Experience so they will fall into a mutually exclusive category.
3. The survey, which is hosted on the AFIT internet, will be available for the survey population.

3.9 Survey Design

Other researchers who have studied the relationship and alignment between a strategic business plan and a strategic information systems plan used Likert scale surveys to collect data (Kearns and Lederer 1999) (Newkirk, Lederer, and Srinivasan, 2003) (Newkirk, Lederer, and Johnson, 2008) (Newkirk and Lederer, 2006) (Kearns and Lederer 2000)and is appropriate for measuring the relationships in this study.

The survey questions are constructed using an interval-level response format commonly referred to as a Likert Scale (Trochim and Donnelly 2008). The questions are constructed in a bipolar format using a scale from one to five (1-5 scale). Using this type of scale allows opinion related responses to be answered negatively, neutral, or positively based upon the respondents' experience (Trochim and Donnelly 2008). The survey is divided into two sections. Section 1 contains demographic information and section 2 contains alignment questions. The survey contains 30 questions mapped to 6 Hypotheses. The survey contains a total of 39 questions if the demographic questions are included in the total count.

Given the population size of 344, and the availability of nearly 100 percent of the populations' email addresses, the whole population will be given access to the survey by way of email directing respondents to a specific website hosted by the Air Force Institute

of Technology. In an attempt to elicit a better response rate, the survey solicitation email was sent from the office of the senior Marine Corp Information Assurance Chief.

The survey was made available to the information assurance community during the 10th annual Information Assurance conference held in Palm Desert, California during the last week of March 2010. The survey responses collected during the conference are combined with the overall survey responses because they are stored within the same database on the hosting web server. The target population at the Communication Chief/Information Assurance conference was people who have a roll in information assurance. Communication Chiefs were offered to take the survey because they manage information assurance personnel within their respective command and have constant managerial oversight of the people working in the information assurance field. The communication chiefs are identified by the MOS 0699 and are either MSgt or MGySgt in rank.

3.10 Survey Bias

To address bias, the intent of offering the survey during the Communication Chief/Information Assurance conference 2010 had a few purposes. First, it was an opportunity to cast a wider net on the information assurance workforce. The conference is a forum where Marine Corps information assurance personnel from all over the world gathered in one location. Second, this was an obvious opportunity to increase response rate for a survey instrument used in a study. Additionally, it seemed like an excellent change to get a richer cross section of the population (Technicians, Middle Managers, and Senior Managers).

3.11 Survey Demographics

Section 1 of the survey consists of demographic questions designed to group respondents into a specific category to analyze different population groups. The category groupings are determined by combining educational level, length of tenure in an information assurance/information security position, years of experience, DoD 8570 technical or management billet level, and organizational level.

Table 6: Demographic Questions

How long have you worked in your current Information Assurance or Network Security billet?	0-3 years	3-7 years	7-10 years	10+ years
What is your highest level of formal education completed?	High School	Undergraduate	Graduate	Post-Graduate
How many years of experience do you have in Information Assurance or Network Security?	0-3 years	3-7 years	7-10 years	10+ years
What is your DoD 8570 IAT billet level?	N/A	IAT level I	IAT level II	IAT level III
What is your DoD 8570 IAM billet level?	N/A	IAM level I	IAM level II	IAM level III
What is your current organization level?	Company	Group/Battalion	Base/Wing/MSC	MEF/Higher HQ

The rank question in table 7 is designed to produce a snapshot of the currently identified information assurance workforce along with the spread of the rank structure of the survey respondents. This snapshot includes military ranks, government employees, contractors, and foreign nationals. Rank is usually correlated to years of experience (Marine Corps Order P1040.31J, DoD 2004). Contractors, however, usually do not fit well within this construct. Therefore, contractors will be grouped according to "How long have you worked in your current Information Assurance or Network Security billet?" Cpl (Corporal) or below is included to identify junior personnel performing information assurance jobs. The lower ranks, including GS-5 (General Service) or

below, usually do not have enough experience or exposure to policy to answer the survey questions presented in this survey. There are exceptions to every rule depending on education and specific billet assignments, however, the grouping of these lower ranks will be for identification purposes. Omitted in the rank question are the ranks of 1stSgt (First Sergeant), SgtMaj (Sergeant Major), and General Officers. First Sergeants and Sergeant's Major are usually filling billets of an administrative and leadership function and therefore usually are not immersed in information policy formulation or enforcement. General Officers and Senior Executive Service (SES) leaders, for the purpose of this survey, are in higher leadership positions and are not the target of this survey. An "Other" category is provided to identify personnel who do not fall into any of the ranks listed.

Table 7: Demographic Questions (Rank)

What is your current rank?	Cpl or below Sgt SSgt GySgt MSgt MGySgt 2ndLt 2ndLt (O1E) 1stLt 1stLt (O2E)	Capt Capt (O3E) Maj LtCol Col GS-5 or below GS-6 or GS-7 GS-8 or GS-9 GS-10 or GS-11	GS-12 or GS-13 GS-14 or GS-15 WO1 CWO2 CWO3 CWO4 CWO5	Contractor Foreign-National Other

The identification of Information Assurance professionals is not specifically codified to a specific Military Occupational Specialty (MOS) within the Marine Corps. The listing of MOS's and civilian occupational codes in table 8 are derived from a message from the office of the Department of the Navy Chief Information Officer released 9 March 2009 titled "Information Assurance and Computer Network Defense

Workforce Improvement Program Implementation Status and CY 2009 Action Plan". These occupational specialty codes include most of the identified personnel performing information assurance duties. The "N/A" and "Other" choice are designed to capture contractors and "other" personnel who are working in an information assurance billet or performing information assurance duties. If a respondent chooses "Other" in the civilian drop down box, they are asked to enter text into a box to identify an MOS, if any, the individual has.

Table 8: Demographic Questions (Occupational Specialty Codes)

What is your primary MOS/Civilian Classification?	Military 0211 0231 0602 0603 0610 0612 0619 0620 0621 0622 0623 0627 0628 0629 0650 0651 0689 0699	Civilian 0332 0334 0335 0340 0343 0390 0391 0392 0854 0855 0856	1410 1411 1421 1550 2203 2204 2210 2611 2621 2629 2631 2821 2823 2847 2862 6694	8846 8055 8848 8858 N/A Other

The survey instrument used in this study targets a wide population ranging from senior leaders (CEO/CIO) to lower level technicians (Computer Security Specialist). Many of the surveys analyzed for this study were targeted at either the CEO/CIO level or senior IS executives (Kearns and Lederer 2000) (Kearns and Lederer 1999) (Newkirk, Lederer, and Srinivasan, 2003) (Newkirk, Lederer, and Johnson, 2008) (Newkirk and

Lederer, 2006) (Burn and Szeto 2000). The demographic question in table 9 is designed to try to identify the civilian equivalent of the respondents' current billet. Identifying and comparing the billets between the private versus public sector companies, specifically within the Department of Defense (DoD), is lacking. The idea is to try to generalize the DoD billets to a civilian equivalent.

Table 9: Demographic Questions (Civilian Equivalent Billet)

What would best describe your civilian equivalent billet?				
Chief Executive Officer (CEO) Chief Information Officer (CIO) Chief Information Security Officer (CISO) Chief Operations Officer (COO) Chief Technology Officer (CTO) Computer Data Entry Operator Computer Data Entry Supervisor Computer Help Desk Supervisor Computer Help Desk Support Computer Operations Director Computer Operations Manager		Computer Operations Supervisor Computer Security Analyst Computer Security Coordinator Computer Security Engineer Computer Security Specialist Computer Systems and Program Director Data Security Analyst Network Communications Technician Network Engineer Network/Data Communications Manager Webmaster		

3.12 Mutual Exclusivity

To ensure each survey respondent is mutually exclusive, there needs to be a way to determine and place each respondent into a specific category. The following table shows these categories and the ranks associated to each category.

Table 10: Rank Categories

Technician	Middle Manager	Senior Manager
Cpl or below	GySgt	MGySgt
Sgt	MSgt	CWO4

SSgt	WO1	CWO5
GS-5 or below	CWO2	Capt
GS-6 or GS-7	CWO3	Maj
YA1	YA2	YA3
YB1	YB2	YB3
YC1	YC2	YC3
Contractor	GS-8 or GS-9	LtCol
Foreign National	GS-10 or GS-11	Col
	2ndLt	GS-12 or GS-13
	1stLt	GS-14 or GS-15

3.13 Data Preparation

Using an Excel spreadsheet, the author developed Visual Basic code within Microsoft Excel (Appendix A), which took all possible combinations of Rank, Mos, and Years of experience to produce all possible valid combinations. These combination were based upon the message from the office of the Department of the Navy Chief Information Officer released 9 March 2009 titled "Information Assurance and Computer Network Defense Workforce Improvement Program Implementation Status and CY 2009 Action Plan"

3.14 Response Validity

The combinations were achieved by separating the enlisted and officer Mos's and using the Marine Corps Mos Manual to determine which rank could be associated with each Mos. The combination of thirty four ranks, four specific categories of years of experience, twenty four enlisted mos's, six officer mos's, three warrant officer mos's, and twenty civilian mos's yielded seven thousand four hundred and eighty (7480) possible combinations. By placing certain MOS and rank restrictions within the calculations, the total possible valid responses came out to be one thousand eight hundred and forty

(1840). These restrictions were necessary because, for example, an officer cannot select and enlisted Mos. Likewise, a government employee with a general schedule (GS) rating cannot select an officer Mos. If a respondent selects a combination that has been determined not to be valid, that specific survey will not be included in the calculation of the responses. A respondent will not be excluded based upon the individuals MOS. The MOS rank, and years of experience are only guides for exclusion. The researcher understands there are exceptions to every rule. If a judgment call is too made, this decision will be annotated within the results section.

The numbers in table11 represent the possible valid demographic combinations a survey respondent could enter based upon the criteria the research established which was based upon the message detailing the mos's most likely involved in dealing with information assurance within the Marine Corps. Determining which category a respondent falls into enables the researcher to make sure each respondent is mutually exclusive.

Table 11: Total Possible Respondent Categories

Category		Percent of Valid		Percent of Total Possibilities		
Technicians	712	0.386956522		0.095187		
Middle Managers	552	0.3		0.073797		
Senior Managers	576	0.313043478		0.077005		
Total Valid	1840	0.245989305				
Total Possibilities	7480					

3.15 Survey Data Analysis

Data were collected using a web based survey. The survey was hosted on a served maintained by the Air Force Institute of Technology at right-Patterson Air Force Base in Dayton Ohio. Each respondent's survey results were maintained in a backend SQL database. When the survey was closed, the researcher was able to retrieve the results from the database via a secure (PKI encrypted) browser only available to the researcher. The results of the entire survey were dumped into an Excel spreadsheet.

The web survey was made available to the information assurance professionals within the Marine Corps from 8 April 2010 until 30 April 2010. In addition of the survey being available via the web, the survey was also available during the 10th annual Marine Corps Information Assurance/Communication Chiefs conference held in Palm Desert, California. This conference was held from 30 March 2010 until 6 April 2010. During this conference, the researcher appealed to the conference attendants to actively participate in this research.

3.16 Survey Questions

Designing the questions used in the survey is gleaned from a publication titled "The effect of strategic alignment on the use of IS-based resources for competitive advantage" (Kearns and Lederer 2000). The first ten questions in the survey are adopted from Kearns and Lederer because they show a dichotomous alignment between the strategic business plan and the strategic information systems plan. These questions are modified slightly for the intended audience. The rest of the questions are slight modifications based upon the previous ten questions. The intent is to show alignment

between the different policies. There are six general hypotheses for this study. Each hypothesis has five questions associated with it for a total of thirty questions.

3.17 Statistical Methods

JMP®® Statistical Discover Software version 8.0.2 by SAS is used to analyze the results of the survey used in this study.

In this study, the researcher adopts the common Greek letters to represent population numerical descriptive measures and Roman letters to represent corresponding descriptive measures for the sample (McClave, Benson and Sincich 2008).

The null hypotheses and alternate hypotheses are stated as either Ha or Hb. The hypotheses are setup this way to show direction of alignment. Ha indicates direction from left to right whereas Hb indicates direction from right to left.

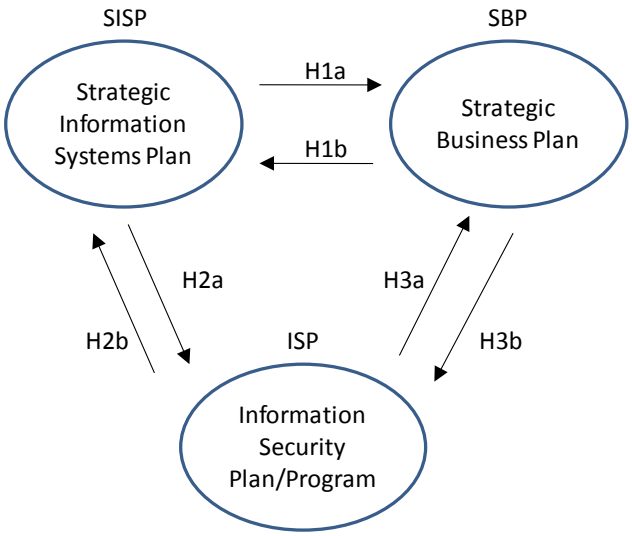

Figure 10: Proposed Model

3.18 Research Hypothesis

3.18.1 Hypothesis 1a:

H_o1a: There is alignment between the Strategic Information System Plan (SISP) and the Strategic Business Plan (SBP).

H_a1a: There is no tendency for alignment between the Strategic Information System Plan (SISP) and the Strategic Business Plan (SBP).

3.18.2 Hypothesis 1b:

H_o1b: There is alignment between the Strategic Business Plan (SBP) and the Strategic Information System Plan (SISP).

H_a1b: The There is no tendency for alignment between the Strategic Business Plan (SBP) and the Strategic Information System Plan (SISP).

3.18.3 Hypothesis 2a:

H_o2a: There is alignment between the Strategic Information System Plan (SISP) and the Information Security Plan (ISP).

H_a2a: There is no tendency for alignment between the Strategic Information System Plan (SISP) and the Information Security Plan (ISP).

3.18.4 Hypothesis 2b:

H_o2b: There is alignment between the Information Security Plan (ISP) and the Strategic Information Systems Plan (SISP).

H_a2b: There is no tendency for alignment between the Information Security Plan (ISP) and the Strategic Information Systems Plan (SISP).

3.18.5 Hypothesis 3a:

H_o3a: There is alignment between the Information Security Plan (ISP) and the Strategic Business Plan (SBP).

H_a3a: There is no tendency for alignment between the Information Security Plan (ISP) and the Strategic Business Plan (SBP).

3.18.6 Hypothesis 3b:

H_o3b: There is alignment between the Strategic Business Plan (SBP) and the Information Security Plan (ISP).

H_a3b: There is no tendency for alignment between the Strategic Business Plan (SBP) and the Information Security Plan (ISP).

3.19 Hypothesis Alpha Level

The level of significance associated with the null hypothesis is set using an alpha of .05 ($\alpha = .05$). The survey instrument used in this research is a likert scale, therefore the data are considered ordinal. Since the author cannot assume the population is normally distributed, a One-way Analysis of Variance (ANOVA) is not suitable for analyzing the results of the survey instrument. The Kruskal-Wallis test is a more

appropriate non-parametric method that uses ranked data to compare three or more groups (Statistics Solutions 2009).

3.20 Kruskal-Wallis

The Kruskal-Wallis test is the nonparametric equivalent to the ANOVA test and uses ranking rather than a mean. The rankings are used for the comparison of the three groups (Technician, Middle Manager, and Senior Manager) to determine if there is a difference in alignment between the groups. The test statistic for the Kruskal-Wallis test is provided in Figure 11: Kruskal-Wallis Test (Higgins 2004).

Figure 11: Kruskal-Wallis Test (Higgins 2004)

The Kruskal-Wallis test is further simplified with the following notation:

Figure 12: Simplified Kruskal-Wallis Test (Higgins 2004)

Where: H = Kruskal-Wallis Test; N = total number of observations in all samples; R_i = Rank of the sample (Statistics Solutions 2009)

The constant twelve (12) represented in the test statistic C=12/N(N+1) is a scaling factor that makes it possible to use the chi-square distribution with k-1 degrees of

freedom to approximate the permutation distribution of Kruskal-Wallis (KW) (Higgins 2004).

There exists the possibility for ties when the raw data is converted into ranked data for analysis by the Kruskal-Wallis method. The adjustment for ties will be handled with the following formula in order to maintain the chi-square approximation.

Figure 13: Kruskal-Wallis test adjusted for ties (Higgins 2004)

3.21 Critical Rejection Value

In order to reject the null hypothesis, the critical rejection value must be defined. The critical values are found in Table B.6 in Corder and Foremans book titled "Nonparametric Statistics for Non-Statisticians" (Corder and Foreman 2009). Referencing Table B.6 on page 232, there are three groups (Technicians, Middle Managers, and Senior Managers) which gives us the value of k=3. The value k represents the number of groups. Since there are three groups associated with each hypothesis and five questions for each hypothesis, this gives the values for n_1, n_2 and n_3, where $n_1 = 5$, $n_2 = 5$, and $n_3 = 5$ respectfully. The critical value for k=3 and 5 5 5 with an alpha of .05 ($\alpha = .05$) yields 5.78 (Corder and Foreman 2009).

The observed value is compared to the critical value to determine if the criterion is met for rejecting the null hypothesis. If the critical value is less than or equal to the obtained value, we must reject the null hypothesis. If the critical value exceeds the obtained value, we do not reject the null hypothesis (Corder and Foreman 2009).

The Kruskal-Wallis test will reveal if there is a significant difference between the three groups in reference to the group means. The Kruskal-Wallis test will not indicate which group is different. To determine which group is different from the other two groups, a different test will have to be applied.

3.22 Mann-Whitney U-test

The test the author uses to determine differences between two samples is called the Mann-Whitney U-test. The Mann-Whitney U-test is a nonparametric statistical procedure for comparing two samples that are independent, or not related (Corder and Foreman 2009). If the results from the Kruskal-Wallis analysis indicate there is a difference among one of the groups, the three groups will be analyzed by comparing the technicians against the middle managers, the middle managers against the senior managers, and the technicians against the senior managers to indicate which group is in fact different.

3.23 Cronbach's Alpha

Internal consistency concerns about the survey questions are answered by conducting the Cronbach's alpha test on the survey questions to ensure they relate to the specific hypothesis in question.

Cronbach's alpha is defined by the following formula: (Gliem and Gliem 2003) (Newkirk, Lederer, and Srinivasan, 2003) (Nunnally 1978)

Figure 14: Cronbach's Alpha formula

Where K = the number of respondents.

= variance of the ith of the current sample.

= variance of the total sample.

There are six hypotheses and thirty questions in the survey instrument. There are six different tests involving Cronbach's alpha test. This test will show if the questions being asked are consistent with the hypothesis. An acceptable Cronbach's alpha score should be above .70 with the goal of reaching at least .80 to ensure the questions are sufficiently measuring the construct (Gliem and Gliem 2003) (Newkirk, Lederer, and Srinivasan, 2003) (Nunnally 1978).

3.24 Summary

This chapter included discussions about research approval, the population of interest, the sample size, response rate, pilot survey, and a few assumptions. The statistical tests used in the study were discussed and explained. Now that we have an understanding of the methods used for this study, we can now focus our attention towards analyzing the results of the survey.

4 Analysis and Results

4.1 Chapter Overview

This chapter presents the results of statistical tests and analysis of the data collected by the procedures outlined in Chapter 3. The data analysis is conducted with a combination of statistical software (SAS JMP® version 8.0.2) and Microsoft® Excel 2008. This presentation is performed in three sections. The first section of this chapter discusses the results of the data preparation and excluded data points. Section two presents the results of the exploratory analysis of respondent demographics. These measures are an important part of the analysis to ensure that the sample is representative of the population since the data can be used to make inferences from the results. Section three presents the results of the statistical tests conducted along with discussion of their practical significance.

4.1.1 Data Preparation

The original uncorrected dataset contained n = 155 responses. Three responses were from validation testing of the online survey. The three responses were deleted from the dataset. Subtracting these administrative test responses provides a corrected dataset of n = 152.

The survey design included rules to distinguish between valid and invalid responses. As indicated in chapter three, a program written in C was implemented during the data preparation stage to identify potential invalid responses is provided in Appendix C.

4.1.2 Invalid Responses

The C program identified three additional entries to exclude from the analysis. Entries identified as items number 14, 25, and 41 were excluded from the data analysis due to invalid responses in the demographics portion of the survey. Table 12 lists the three additional entries excluded from data analysis.

Table 12: Invalid survey responses

Item#	Experience	Rank	Rank Other	MOS	MOS Other
14	7-10 Years	N/A	Contractor	0689	N/A
25	0-3 Years	N/A	GS-14 or GS-15	Other	Education
41	0-3 Years	GySgt	N/A	Other	N/A

Item number 14 is the first invalid demographic response. Table 12 shows the respondent selected “contractor” for a “rank other” with an invalid occupation “MOS” (Military Occupational Specialty) code of “0689”. Contractors cannot have an MOS since they are not military members (Marine Corps Order P1040.31J, DoD 2004). This combination does not allow the respondent to be assigned to a mutually exclusive group for data analysis.

Item number 25 is the second invalid demographic response in Table 12 shows the respondent selected “GS-14 or GS-15” for a “rank other” with an invalid “MOS other” occupational code of “education”. The combination does not allow the respondent to be assigned to a mutually exclusive group for data analysis. Item number 41 is the third invalid demographic response. Table 12 shows the respondent selected “GySgt” for a “rank” but did not specify a valid Military Occupational Specialty (MOS) or “MOS

Other". This combination does not allow the respondent to be assigned to a mutually exclusive group for data analysis.

The remainder of the entries all contained valid responses in the demographic section. Additionally, the survey questionnaire all contained valid entries (e.g. a single response per entry and no missing responses).

The total corrected number of responses available for data analysis is n = 149. This represents 96% of the original data. The corrected respondent data was imported to Microsoft Excel® 2008 and JMP® for further data analysis.

4.2 Survey Response Rate

The collection method used was a combined hybrid approach of an online survey and person-to-person solicitation at a conference to participate in the online survey. The results of each individual collection method fell below expected values for either method individually. The web survey method attracted 77 respondents and yielded a 22.38% response rate. The conference survey method collected 72 responses which yielded a 20.93% response rate. Combining these collection methods to produce a total of n = 149 survey respondents yielded a response rate of 43.31%. This total value exceeds an expected web survey response rate of 32.52% (Hamilton 2009) and an expected response rate of 41.21% for populations less than 1000 (Gay, 1989). Table 13 provides the allocation of the survey collection methods.

Table 13: Allocation of survey methods

Method	Quantity	Expected	Results
Web Survey	77	32.52%	22.38%
Conference	72		20.93%
	149	41.21%	43.31%

All surveys, which are publically accessible and hosted on Wright-Patterson Air Force base websites, must get approval from the 88th Force Support Squadron public affairs office. A public affairs request was submitted and approved on 18 December 2009. The following public affairs case number was assigned: 88ABW-2009-5210.

4.3 Instrument Reliability

Internal consistency is an important factor for ascertaining if items can reliably measure the latent construct under consideration. Intercorrelations among test items are maximized when all items measure the same construct. Cronbach's alpha is widely believed to indirectly indicate the degree to which a set of items measure a single unidimensional latent construct.

A minimum level of acceptance is considered to be a Cronbach's value above .70 (Gliem and Gliem 2003) (Newkirk, Lederer, and Srinivasan, 2003) (Nunnally 1978). One question, (SEC2_Q26_INFOSECPLAN_REF_OPPLAN) was the only question below the .70 range. Referencing the above authors, anything below .60 should be questioned. The specific question falling below .70 by itself should not be a cause for alarm since it is on the boundary of the suggested cutoff point.

Tables 14, 15, and 16 provide Cronbach's alpha tests related to each hypotheses. The results were calculated using JMP® version 8.0.2 by applying the following formula:

Figure 15: Cronbach's alpha formula

Table 14 indicates each item with an associated score grouped by hypothesis 1a and 1b. The label 'Entire Set' refers to the Cronbach's alpha score of the 5 items that are grouped under each hypothesis and is not calculated as an average of the combined alpha scores.

Table 14: Cronbach's alpha for hypothesis 1a and 1b

Hypothesis	Question	α	Hypothesis	Question	α
H1a	1	0.777	H1b	1	0.848
	2	0.768		2	0.818
	3	0.796		3	0.823
	4	0.774		4	0.824
	5	0.907		5	0.862
	Entire Set	0.837		Entire Set	0.864

The results of 1a and 1b indicate the items in the survey measure the intended hypothesis adequately.

The results of Cronbach's alpha for hypothesis 2 in Table 15 indicate that all of the items adequately measure the intent of hypothesis for hypothesis 2a and 2b.

Table 15: Cronbach's alpha for hypothesis 2a and 2b

Hypothesis	Question	α	Hypothesis	Question	α
H2a	1	0.877	H2b	1	0.824
	2	0.877		2	0.831
	3	0.887		3	0.828
	4	0.877		4	0.863
	5	0.919		5	0.904
	Entire Set	0.908		Entire Set	0.877

Hypothesis 3a in Table 16 has a strong score indicating these questions are measuring the intended hypothesis. Hypothesis 3b, although indicating a lower score than the rest of the displayed scores, still scores above the minimum level of acceptance according to Cronbach's alpha.

Table 16: Cronbach's alpha for hypothesis 3a and 3b

Hypothesis	Question	α	Hypothesis	Question	α
H3a	1	0.799	H3b	1	0.693
	2	0.808		2	0.703
	3	0.795		3	0.726
	4	0.806		4	0.770
	5	0.922		5	0.748
	Entire Set	0.860		Entire Set	0.770

The items presented for hypothesis 2 and 3 were modeled in the same format as items from hypothesis 1. These questions were also the first of its kind in measuring these types of questions. The fact that the 'Entire Set' scores were all above .70 shows these questions were designed correctly. Inferences from the results of these questions are therefore valid.

A prudent decision was made no to inflate the number of questions in the scale as this might inadvertently increase the Cronbach's alpha result. Questions were reviewed during the pilot study to minimize question redundancy as this could also lead to high

Cronbach's alpha values. In conclusion, the result of the Cronbach's alpha values for each hypothesis provides sufficient confidence that the instrument is reliably measuring the latent construct for each hypothesis presented.

4.4 Demographic Analysis

In this section, descriptive statistics will be presented to further evaluate the sample. Elements of data collected from the demographics portion of the instrument such as Work experience, education level, Certification levels, and job specialties will be graphically presented and discussed.

4.4.1 Work Experience

A comparison of work experience is represented in Figure 16: Work Experience. The category of 0-3 year's shows there are more personnel with 0-3 years of experience working in job positions. This is typical in the Marine Corps. The attrition rate for an average job position within a command is about three years. There seems to be an even tie for 3-7 years. The average years of experience equals the total years of experience. These results suggest that about 24% of the workforce are working in job positions for 3-7 years with an average of 3-7 years total experience.

As the IA workforce matures and gets promoted, career overtakes position because the average position is three years but the years accumulated towards a career are continuous. Looking at the 10+ year category, it appears that the longer the career, the long a person stays within a certain job position. This could be explained by the difficulty of placing higher or senior level personnel in specific job positions. Casual

discussions with people who wish to remain anonymous say part of this problem lies with moving every three years. Moving senior personnel usually involves uprooting a family, changing schools for kids, issues dealing with buying and selling a house, and other life changing events non-military people only do once in their life.

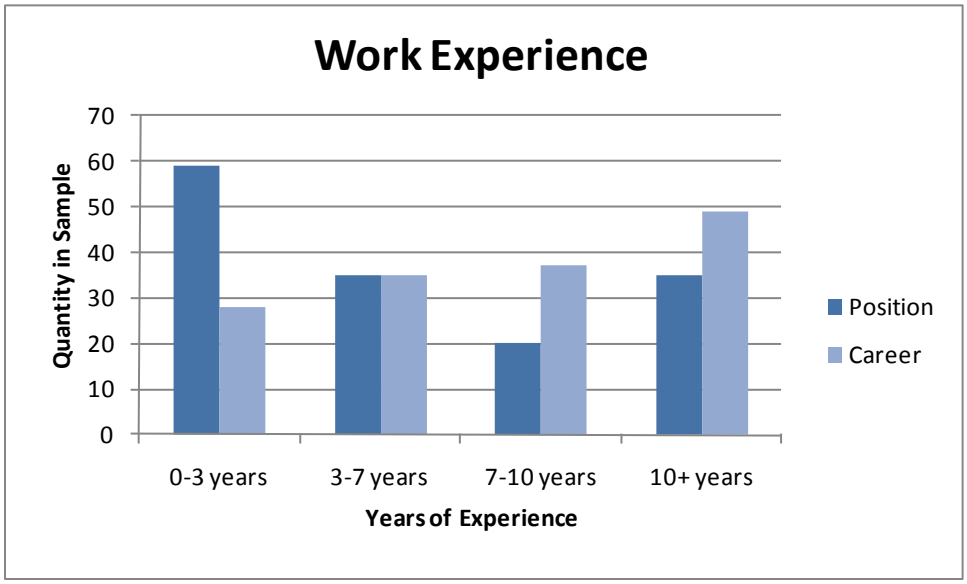

Figure 16: Work Experience

Junior personnel working in the 0-3 year category, as expected, have less experience. Personnel working in the 3-7 year category tended to have about the same amount of job position experience as career experience. The more seniority a person obtains, the trend seems to level off. Personnel in the 7-10 years and 10+ year's category naturally have more career experience than billet experience.

4.4.2 Education Level

The first category of Figure 17: Respondents Education Level is common among the Marine Corps. The survey asked respondents to select the highest level of education.

Commonly within the Marine Corps, the enlisted community rank higher in high school as the highest education level. An important note to point out in the first category is the one officer that selected high school. Traditionally, officers need a bachelor's degree to obtain a commission; however, within the Marine Corps the warrant officer community does not require a higher education. The undergraduate, or the first four years of college, shows a tie between the enlisted community and the civilian workforce.

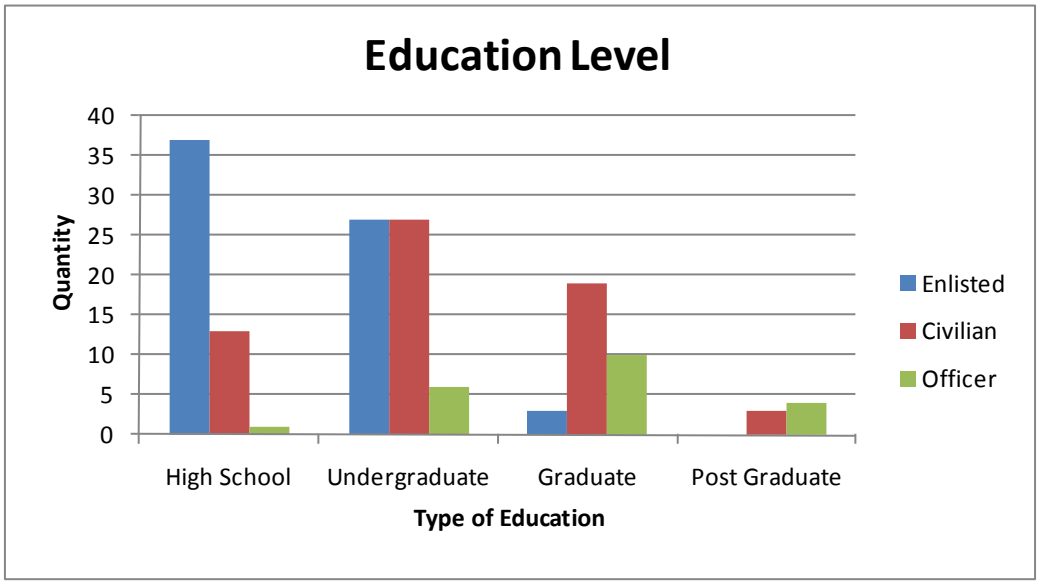

Figure 17: Respondents Education Level

The results of this survey indicate that 18% of the enlisted have at least a bachelor's degree. The average of enlisted with bachelor's degree in Figure 17: Respondents Education Level shows 1.41%. This observation suggests more of the enlisted in the information assurance community are seeking continuing education.

Due to the highly technical nature of the information assurance community, the information assurance workforce is exposed, and in many cases, required to attend many

training sessions relating to their specific job or billet compared to other communities within the Marine Corps. This constant training, education exposure, and educational opportunities may explain why more of the enlisted are seeking higher levels of education.

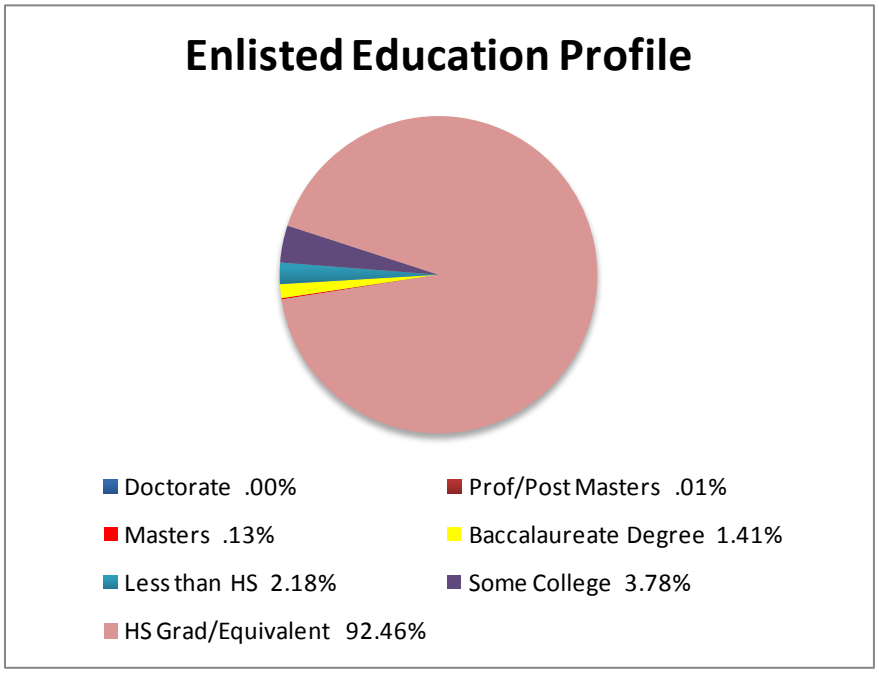

Figure 18: Marine Corps Enlisted Profile (Headquarters Marine Corps, 2008)

The results of the officers follow the expected trend. The longer an officer stays in the Marine Corps, the higher level of education he/she obtains. Within the officer community, education is heavily considered for promotions. The results from the survey are representative according to the latest Marine Corps education statistics referenced in Figure 18: Marine Corps Enlisted Profile (Headquarters Marine Corps, 2008).

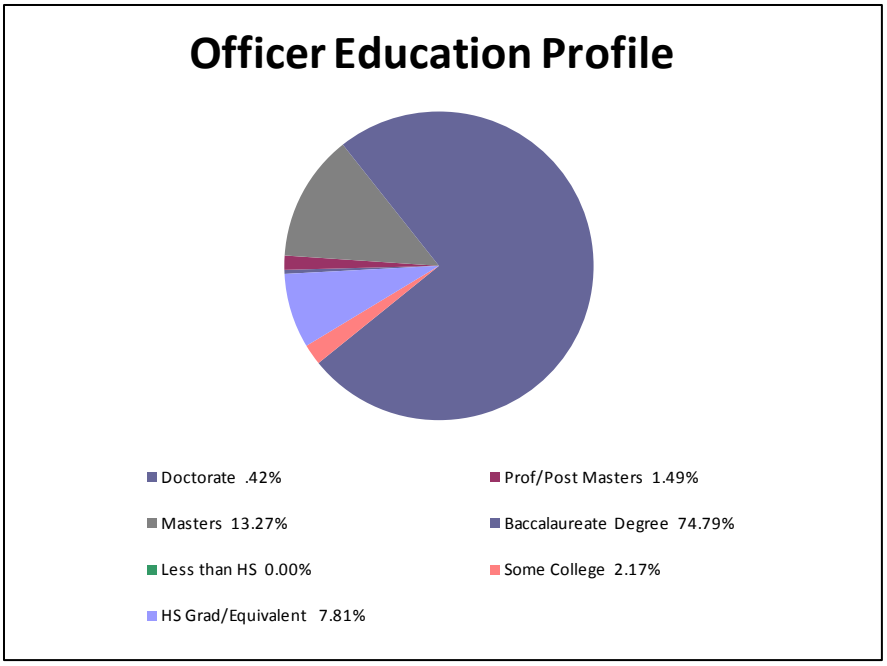

Figure 19: Marine Corps Officer Education Profile (Headquarters Marine Corps, 2008)

The researcher could not obtain comparisons for the average education level of civilians in the Department of Defense or within the Marine Corps. Without information about the average DoD civilian education level, a comparison could not be established.

4.4.3 DoD 8570 Certification Levels

The following figure indicates the self reported Information Assurance Technician (IAT) and Information Assurance Manager (IAM) levels. The researcher discovered a potential questionable problem area when analyzing the data. The potential problem questions are the two survey demographic questions which asked respondents 'What is your DoD 8570 (IAT or IAM) billet level?'. The survey questions were not designed to be mutually exclusive. This allowed the respondents to select both IAT and

IAM. An assumption is that respondents chose the IAT and IAM levels that correspond to their certification level. If the sample population were polled, some of the population would possibly reference the current version of DoD 8570. DoD 8570.01M states the following:

> C2.2.5. A position may include functions spanning multiple levels. In these cases, the level, and related certification requirements will be those of the highest level functions. Individuals performing functions in multiple categories or specialties must hold certifications appropriate to the functions performed in each category or specialty. (Note: one certification may cover more than one category or specialty and level, (e.g., a Security + certification can qualify someone to fill both an IAT-I and an IAM-I position.) (DoD 8570.1M: Information Assurance Workforce Improvement Program 2008)

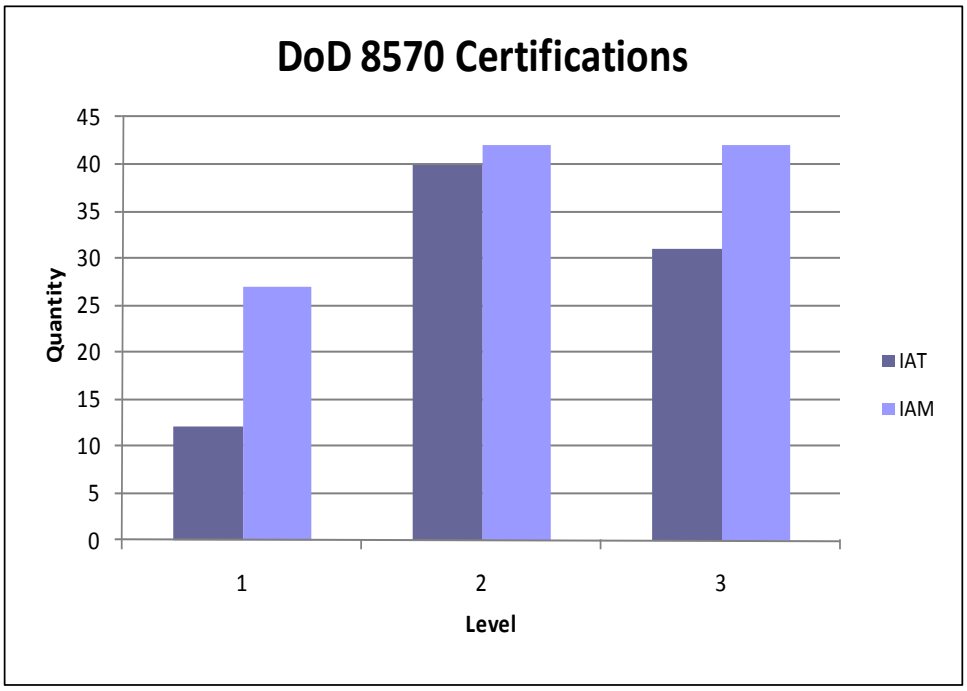

Figure 20: DoD 8570 Certification Levels

Due to the question represented in Figure 20 not being mutually exclusive, there could be some self reporting bias in the answers obtained. The researcher expected to see

more IAT responses within the Level 1 category. Level 1 in the chart represents the Technician grouping. Level 2 represents the Middle Managers and Level 3 represents Senior Managers.

To further understand the demographic responses of the IAT and IAM certification levels, the following figures are different representations separated by Military, Civilian, and Contractor.

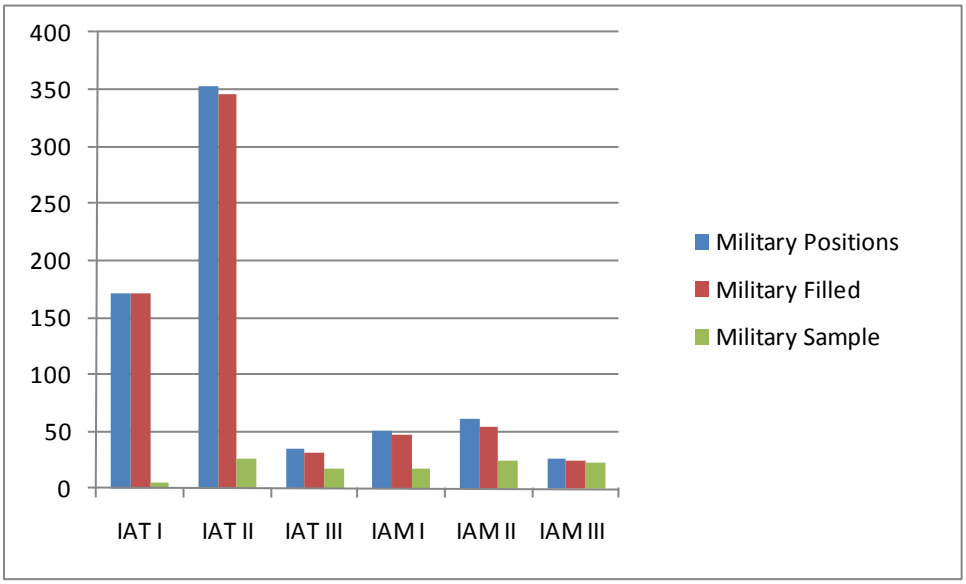

Figure 21: Military IAT/IAM Levels

The representation in Figure 19 show only the military positions, the military positions filled, and the responses received from the survey. This information was obtained from an internal For Official Use Only (FOUO) Marine Corps report (Annual Information Assurance Workforce Quantitative Report). This report is required by DoD 8570.01M and mandated by the Federal Information Security Management Act (FISMA). According to the chart, the IAT levels are underrepresented in this sample

according to the positions available and positions filled. The chart appears to be leaning to the right with a large percentage of the respondents choosing higher IAM levels. Perhaps another assumption is that respondents chose the higher IAM levels in an attempt to elevate one's own sense of stature or self worth. The physiological explanation is well beyond the context of this research.

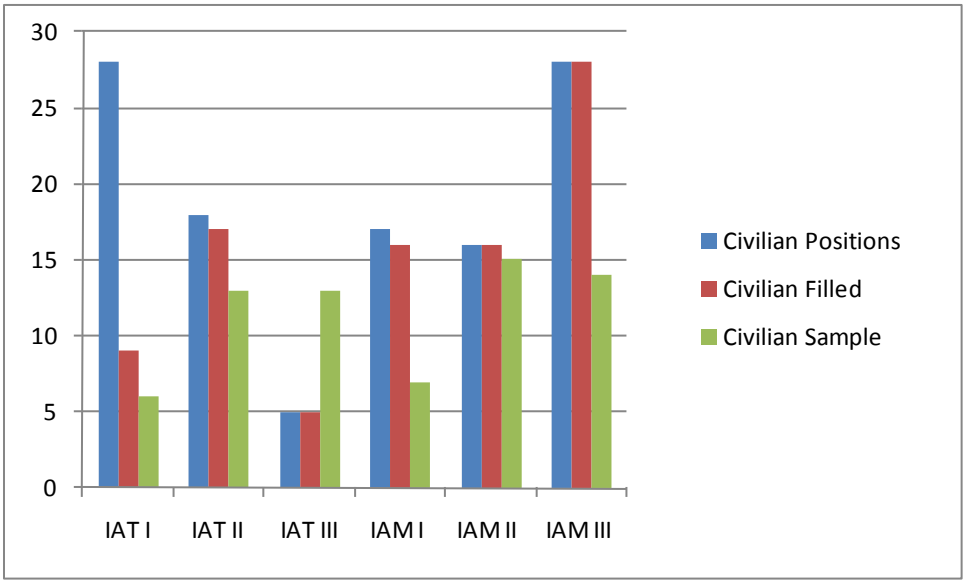

Figure 22: Civilian IAT/IAM Levels

The civilian respondent breakdown shows a very interesting data point. Attention should be drawn to the IAT III. The official reported positions of IAT level III are five with five positions currently filled (as of December 2009). The reported IAT III level is almost three times more than the positions available. This appears to be associated with the mutually exclusive problem with the question. The researcher believes the respondents chose the highest IAT/IAM level associated with their certification level. The intent of the question was to determine how many people were working in billets that

required a specific IAT or IAM level. Each IAT or IAM billet within the Marine Corps is supposed to be assigned in writing according to (DoD 8570.1M: Information Assurance Workforce Improvement Program 2008).

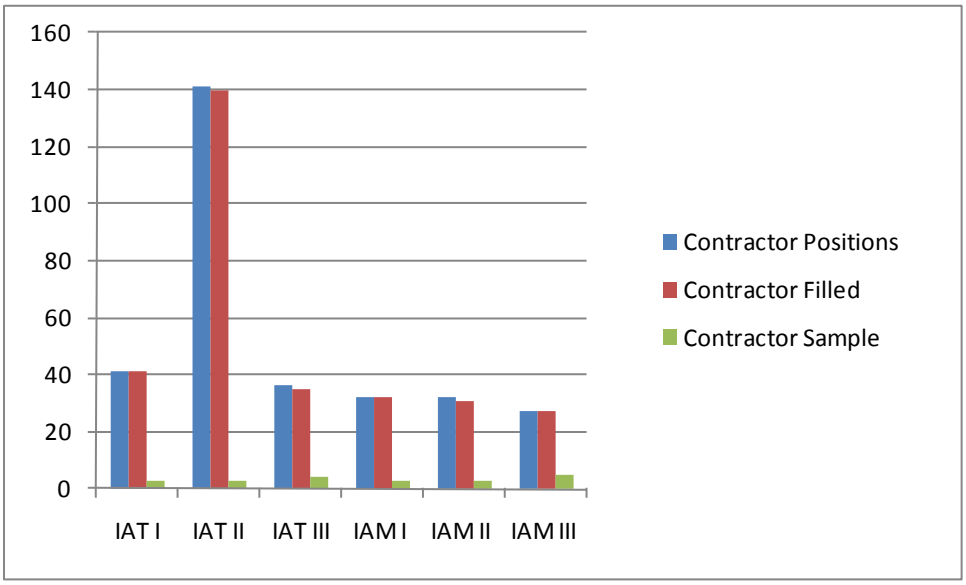

Figure 23: Contractor IAT/IAM Levels

The contractor levels were very low according to the available positions and filled positions compared to the reported numbers from the survey.

The questions should be worded to allow the respondent to choose 'the highest IAT or IAM level' that ties to the individuals specific billet and be limited to the specific billet the respondent is occupying.

4.4.4 Rank

The following breakouts represent the distribution of the ranks of the survey respondents. The first figure shows the split of respondents by rank.

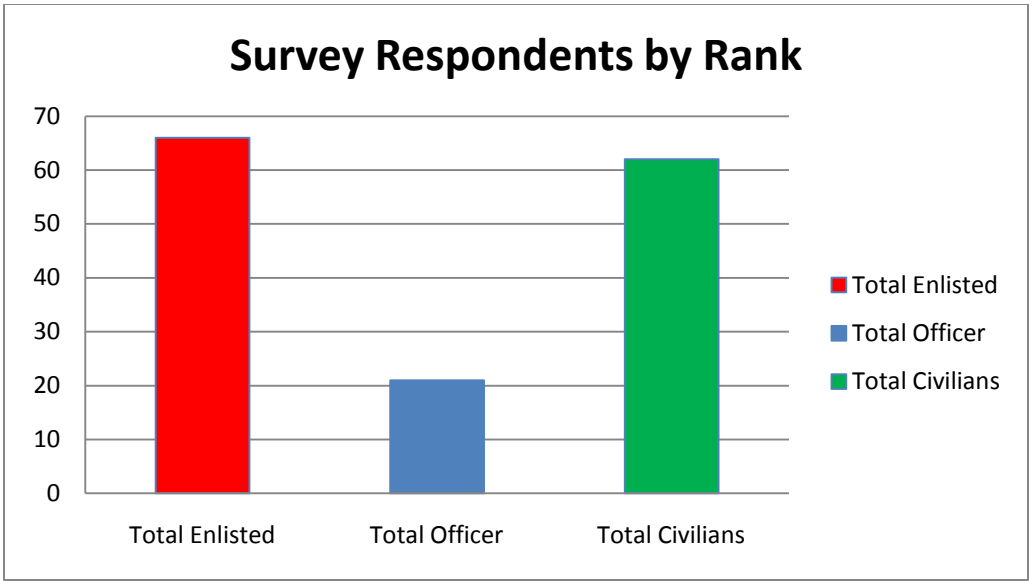

Figure 24: Respondents by Rank

There was almost a split of enlisted versus civilian survey respondents. The enlisted total was 66 which calculate to 44% while the civilian total was 62 which calculate to 42%. The civilian population constructed of contractors and government employees. The officer population came in last with a representation of 21 which calculated to 14%.

Figure 25: Enlisted Response by Rank displays the enlisted rank distribution. The enlisted rank distribution shows a representative sample of the enlisted population of the information assurance workforce. Total enlisted response represented 43% of the survey response rate and represents 85% of the Marine Corps Information Assurance Workforce. There are 78 enlisted personnel listed in the Marine Corps IA contacts list from which the sample population was targeted.

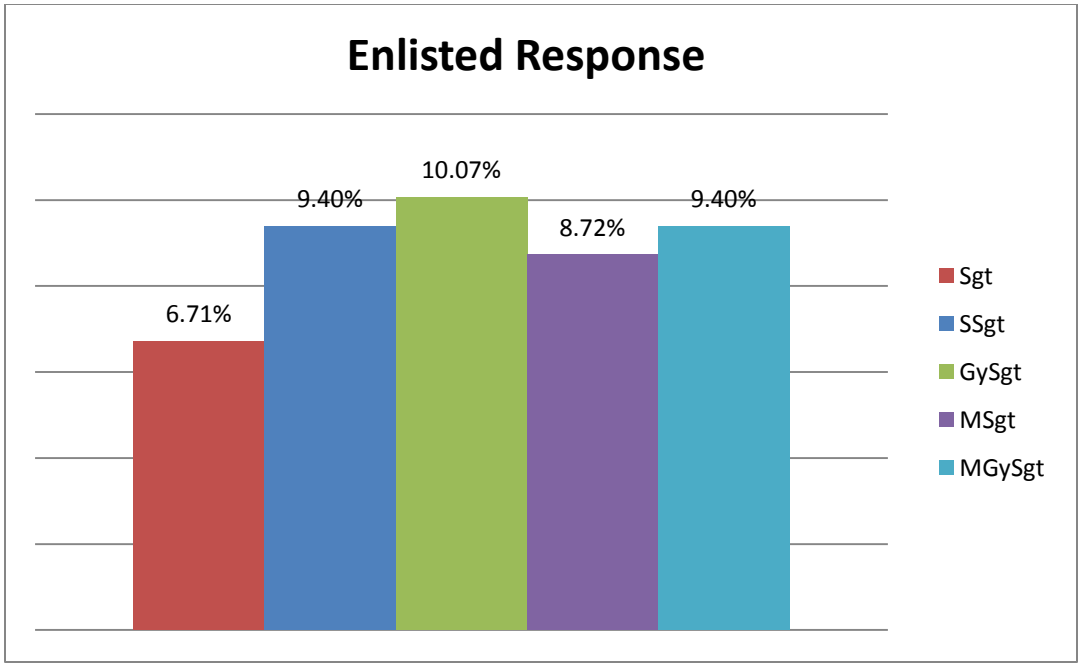

Figure 25: Enlisted Response by Rank

The officer rank distribution shows a good representation of officers who responded to the survey. The overall officer representation calculated to 14%.

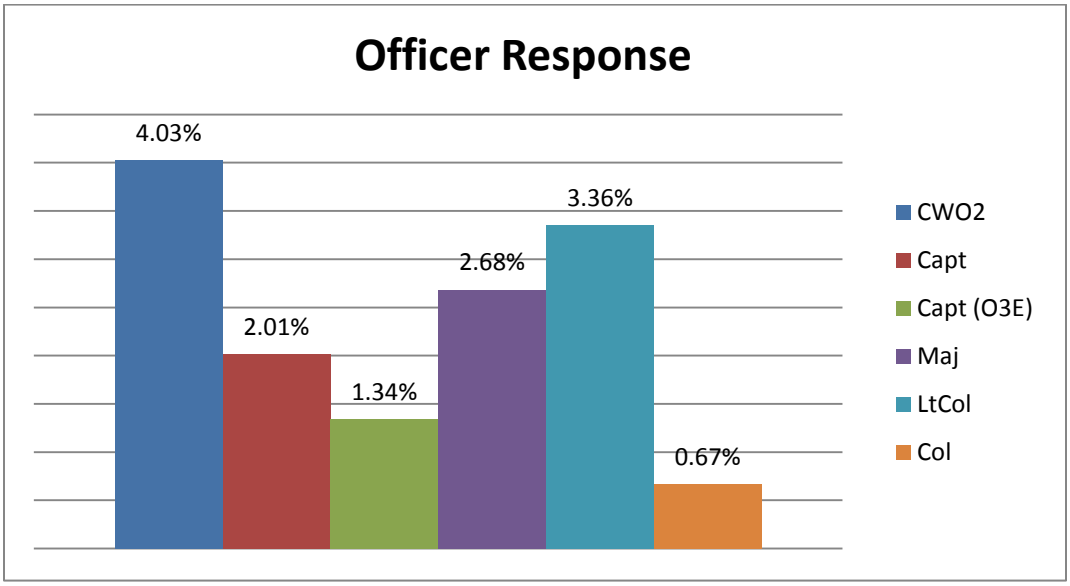

Figure 26: Officer Response by Rank

Referencing the Marine Corps Information Assurance Workforce, the officer response made up 41% of the IAW representing 21 out of the 51 listed in the IAW. The civilian response rate represents almost 42% of the survey response rates. There is a good representation of the civilian workforce in the results. These results also indicate capturing about 43% of the IAW.

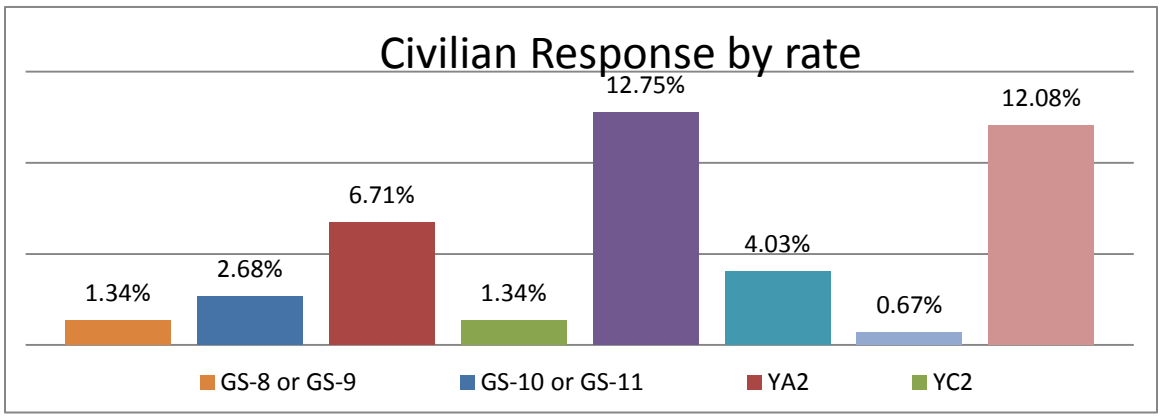

Figure 27: Civilian Response by Rate

Overall, there is a sufficient spread of ranks in the dataset that coincide with the three levels being analyzed. The three groups, Technician, (Middle Manager, and Senior Manager), are well represented. Determining the rank distribution seem to be fair, this reduces the bias of the results of the hypotheses.

4.4.5 MOS breakdown

Just like the rank breakdown, the MOS breakdown shows a good representation of the MOS's across the Marine Corps. Starting with the officer MOS's and the civilian specialty codes, there is a wide range of different job codes present. Since there were more civilian responses than officer responses, it would follow that 2210 (a civilian

specialty code) has the strongest representation. DoD contractors also had a strong showing. The officer MOS's, although showing small numbers here, represent almost 40% of the IAW.

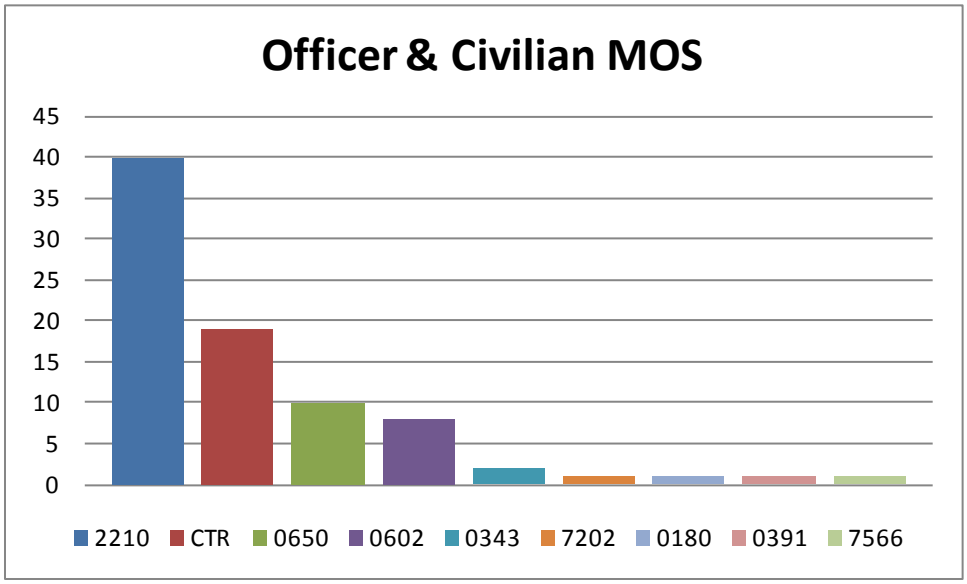

Figure 28: Officer and Civilian MOS

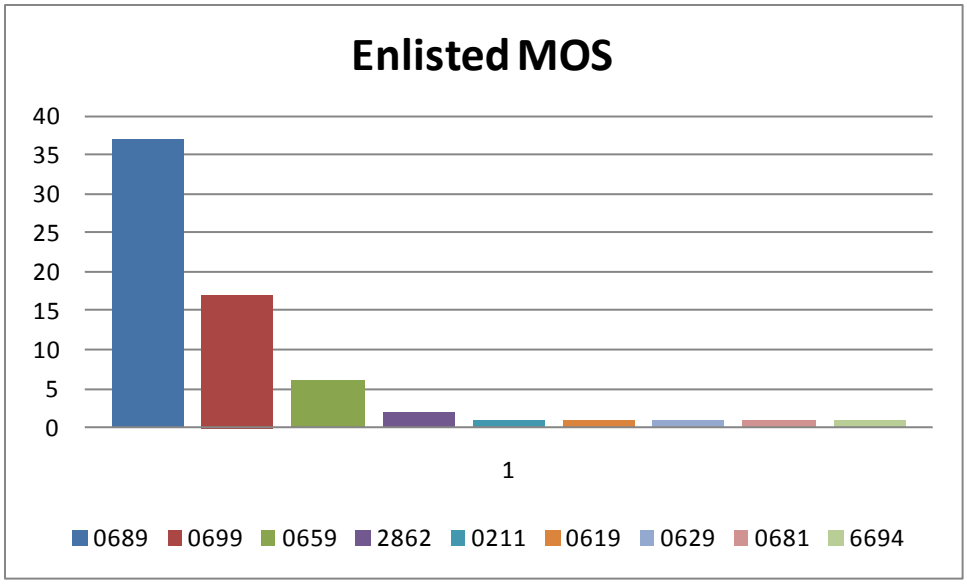

Figure 29: Enlisted MOS

The enlisted MOS spread shows a good representation of enlisted Marines who indicated they perform information assurance functions. Special attention should be drawn towards the 0699 (Communication Chiefs). The attendance of the Communication Chiefs at the 10th annual Information Assurance Conference was the first time the Communication Chiefs attended a conference concurrently with the information assurance workforce. The relationship between the information assurance community and the Communication Chiefs has matured over the past few years to the point that both communities now understand more of how each community operates. In the past, these communities were separated and animosity and the relationships were full of tension. The Communication Chiefs are the leaders of the communication field and have the ability to stifle the progress of the information assurance community. Information assurance professional were impeded because of a lack of understanding of what each

community was trying to achieve. The information assurance community, at the same time, shot itself in the foot by trying to act independently without the consent and/or support from the Communication Chiefs. These relationships have matured over the past few years and now both communities are working together to provide better support.

The analysis of years of experience, education, IAT/IAM levels, rank, and MOS represent an accurate account of the demographics. With an understanding of the demographics, the attention is now focused on analyzing the hypotheses.

4.5 Hypothesis Testing

In the following section, the hypotheses are analyzed using the nonparametric Kruskal-Wallis test statistic to rank the sum of the responses. The layout for the hypothesis analysis will be standard for all six hypotheses. The null hypothesis will be declared followed by the alternative hypothesis. The test statistic will be stated. The criteria for rejecting the null hypothesis will be the stated, although it will be the same for all sic hypotheses. Finally, the critical value will be stated. The critical value is the same as the Chi-square approximation. The p value will also be included to show if the observed value is above or below the α level. The α level is set to .05.

The output from JMP® version 8.0.2 includes a figure and table for each hypothesis. The figure is a pictorial representation of the results. The X-axis is numbered as 1, 2, and 3. These numbers represent the Group ID. The Group ID's are the three mutually exclusive groups with Technician = 1, Middle Manager = 2, and Senior Manager = 3. The Y-axis represents the question Likert response scale from the survey. The Likert response scale starts at 1 and continues to 5. The average responses for the

five questions associated with each hypothesis are represented as diamonds with box plots overlaying the diamonds to show where the average responses show up. An outlier is identified as a middle manager (Group ID 2) where a respondent answered 1 (Strongly Disagree) for all questions. There was no justification however to exclude this data point.

The table shows the statistical results from the Kruskal-Wallis test. The level represents the specific groups. The count shows the response composition of each group. The more important numbers in this table is the ChiSquare approximation and the probability of ChiSquare.

4.5.1 Hypothesis 1a Analysis

H_o = there is alignment between the Strategic Information System Plan (SISP) and the Strategic Business Plan (SBP).

H_a = alignment is not present.

Test statistic: ———

Rejection Region: Reject H_o if $H < 5.780$.

Critical Value: $H = 2.918$ ($p = 0.232$)

Figure 30: JMP® output for Hypothesis 1a shows that the technicians and middle managers have the same feeling about the alignment between the Strategic Information System Plan (SISP) and the Strategic Business Plan (SBP). The senior managers feel stronger about this relationship.

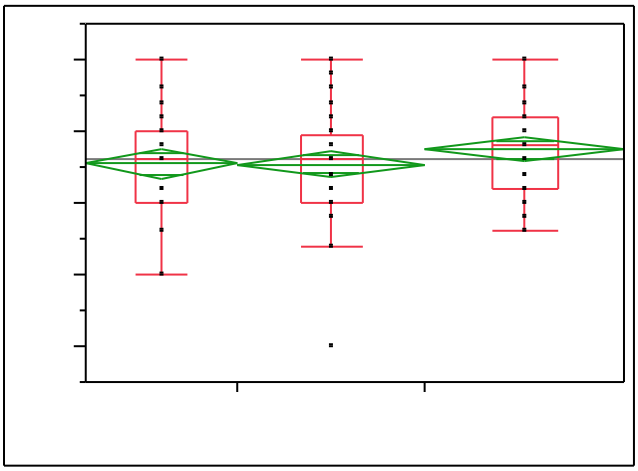

Figure 30: JMP® output for Hypothesis 1a

Table 17 shows the score sum, score mean, and standard deviation of each groups' response. The standard deviations are close for each groups' response indicating most of the population answered about the same.

Table 17: JMP® output for Hypothesis 1a

The observed Kruskal-Wallis value of 2.918 is below the critical value of 5.78, therefore the null hypothesis fails to reject. The results indicate that all three groups (Technicians, Middle Managers, and Senior Managers) believe there is alignment between the Strategic Information System Plan (SISP) and the Strategic Business Plan (SBP). Technicians and the Middle Managers answered about the same for this hypothesis with only a two point difference in mean scores.

The literature supports the alignment from a strategic information systems plan to the strategic business plan (Kearns and Lederer 2000) (Gottschalk 1999). In the context of the survey, this alignment was measured by how well the Communication Plan (Comm Plan) was aligned with the Operation Plan (OPLAN).

4.5.2 Hypothesis 1b Analysis

H_o = there is alignment between the Strategic Business Plan (SBP) and the Strategic Information System Plan (SISP).

H_a = alignment is not present.

Test statistic: ———

Rejection Region: Reject H_o if $H < 5.780$.

Critical Value: $H = 1.866$ ($p = 0.910$)

The observed Kruskal-Wallis value of 1.866 is below the critical value of 5.78, therefore the null hypothesis fails to reject. The results indicate that all three groups (Technicians, Middle Managers, and Senior Managers) believe there is alignment between the Strategic Business Plan (SBP) and the Strategic Information System Plan (SISP). The literature supports the alignment from the Strategic Business Plan to a

Strategic Information Systems Plan (Kearns and Lederer 2000) (Gottschalk 1999). In the context of the survey, this alignment was measured by how well the Operation Plan (OPLAN) was aligned with the Communication Plan (Comm Plan).

Figure 31: JMP® output for Hypothesis 1b shows that the all three groups have the same feeling about the alignment between the Strategic Business Plan (SBP) and the Strategic Information System Plan (SISP).

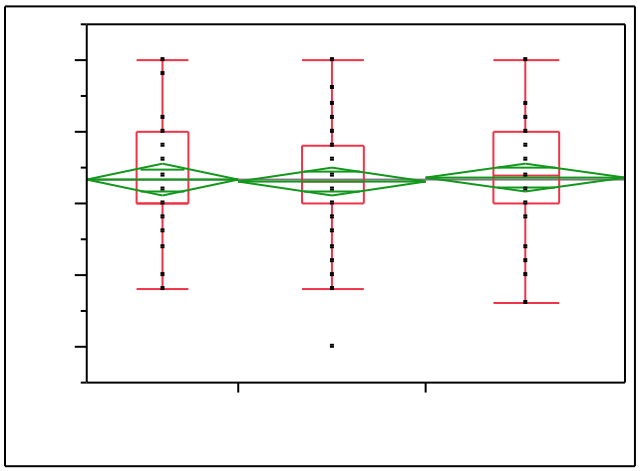

Figure 31: JMP® output for Hypothesis 1b

Table 18 shows the score sum, score mean, and standard deviation of each groups' response. The standard deviations are close for each groups' response indicating most of the population answered about the same.

Table 18: JMP® output for Hypothesis 1b

4.5.3 Hypothesis 2a Analysis

H_o = there is alignment between the Strategic Information System Plan (SISP) and the Information Security Plan (ISP).

H_a = alignment is not present.

Test statistic: ——

Rejection Region: Reject H_o if $H < 5.780$.

Critical Value: $H = 1.619$ ($p = 0.445$)

The observed Kruskal-Wallis value of 1.619 is below the critical value of 5.78, therefore the null hypothesis fails to reject.

Figure 32: JMP® output for Hypothesis 2a shows there is a gradual increase about the feeling of alignment between the Strategic Information System Plan (SISP) and the Information Security Plan (ISP). Although all three groups feel there is alignment, the technicians feel this alignment is not as strong as the senior managers. This could be due to technicians performing the hands on portion of the plan compared to the planning that takes place at higher levels.

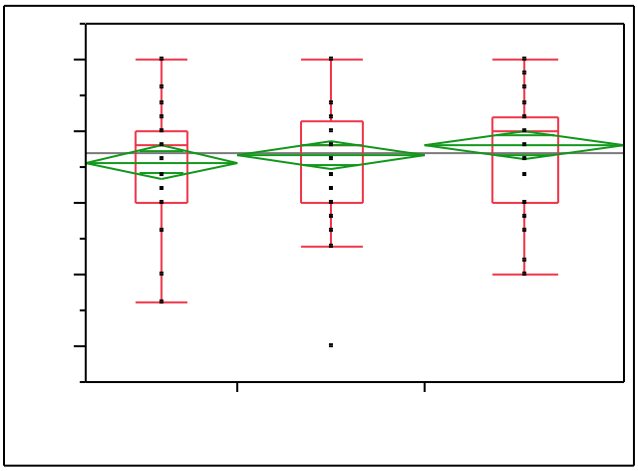

Figure 32: JMP® output for Hypothesis 2a

Table 19 shows the score sum, score mean, and standard deviation of each groups' response. The standard deviations are close for each groups' response indicating most of the population answered about the same.

Table 19: JMP® output for Hypothesis 2a

The results indicate that all three groups (Technicians, Middle Managers, and Senior Managers) believe there is alignment between the Strategic Information System Plan (SISP) and the Information Security Plan (ISP). In the context of the survey, this

alignment was measured by how well the Communication Plan (Comm Plan) was aligned with the Information Security Plan (ISP).

4.5.4 Hypothesis 2b Analysis

H_o = there is alignment between the Information Security Plan (ISP) and the Strategic Information System Plan (SISP).

H_a = alignment is not present.

Test statistic: ———

Rejection Region: Reject H_o if $H < 5.780$.

Critical Value: $H = 1.519$ ($p = 0.467$)

The observed Kruskal-Wallis value of 1.519 is below the critical value of 5.78, therefore the null hypothesis fails to reject.

The results indicate that all three groups (Technicians, Middle Managers, and Senior Managers) believe there is alignment between the Information Security Plan (ISP) and the Strategic Information System Plan (SISP). In the context of the survey, this alignment was measured by how well the Information Security Plan (ISP) was aligned with the Communication Plan (Comm Plan).

Figure 33: JMP® output for Hypothesis 2b shows that the all three groups have the same feeling about the alignment between the Information Security Plan (ISP) and the Strategic Information System Plan (SISP).

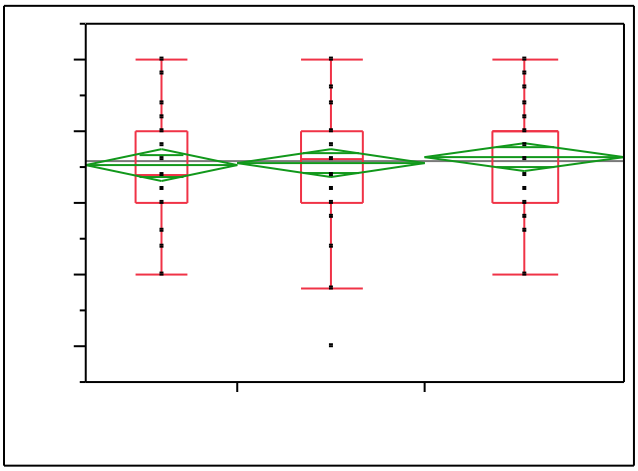

Figure 33: JMP® output for Hypothesis 2b

Table 20 shows the score sum, score mean, and standard deviation of each groups' response. The standard deviations are close for each groups' response indicating most of the population answered about the same.

Table 20: JMP® output for Hypothesis 2b

4.5.5 Hypothesis 3a Analysis

H_o = there is alignment between the Information Security Plan (ISP) and the Strategic Business Plan (SBP).

H_a = alignment is not present.

Test statistic: ———

Rejection Region: Reject H_o if $H < 5.780$.

Critical Value: $H = 3.162$ ($p = 0.205$)

The observed Kruskal-Wallis value of 3.162 is below the critical value of 5.78, therefore the null hypothesis fails to reject.

The results indicate that all three groups (Technicians, Middle Managers, and Senior Managers) believe there is alignment between the Information Security Plan (ISP) and the Strategic Business Plan (SBP). In the context of the survey, this alignment was measured by how well the Information Security Plan (ISP) was aligned with the Operation Plan (OPLAN).

Figure 34: JMP® output for Hypothesis 3a shows that the all three groups have the same feeling about the alignment between the Information Security Plan (ISP) and the Strategic Business Plan (SBP).

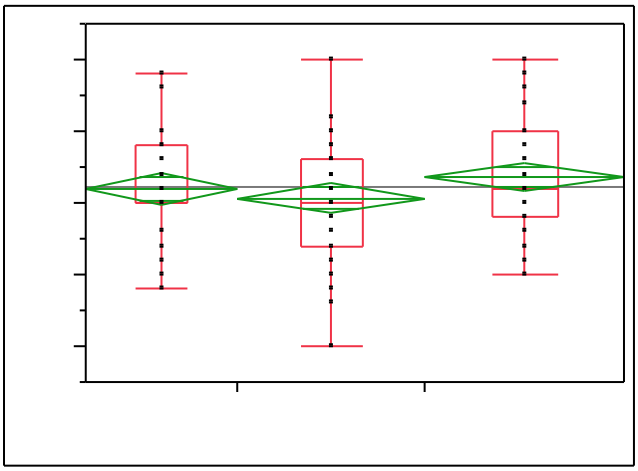

Figure 34: JMP® output for Hypothesis 3a

Table 21 shows the score sum, score mean, and standard deviation of each groups' response. The standard deviations are close for each groups' response indicating most of the population answered about the same.

Table 21: JMP® output for Hypothesis 3a

4.5.6 Hypothesis 3b Analysis

H_o = there is alignment between the Strategic Business Plan (SBP) and the Information Security Plan (ISP).

H_a = alignment is not present.

Test statistic: ———

Rejection Region: Reject H_o if $H < 5.780$.

Critical Value: $H = 1.423$ ($p = 0.490$)

The observed Kruskal-Wallis value of 3.162 is below the critical value of 5.78, therefore the null hypothesis fails to reject.

The results indicate that all three groups (Technicians, Middle Managers, and Senior Managers) believe there is alignment between the Strategic Business Plan (SBP) and the Information Security Plan (ISP). In the context of the survey, this alignment was measured by how well the Operation Plan (OPLAN) was aligned with the Information Security Plan (ISP).

Figure 35: JMP® output for Hypothesis 3b shows that the all three groups have the same feeling about the alignment between the Strategic Business Plan (SBP) and the Strategic Information System Plan (SISP).

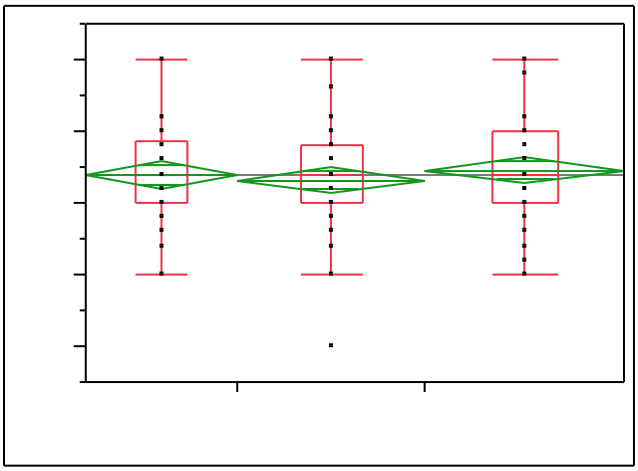

Figure 35: JMP® output for Hypothesis 3b

Table 22 shows the score sum, score mean, and standard deviation of each groups' response. The standard deviations are close for each groups' response indicating most of the population answered about the same.

Table 22: JMP® output for Hypothesis 3b

4.5.7 Investigative Questions Answered

The addition of the ISP construct to the existing model appears to be already existent but not necessarily realized. The results of the survey suggest that security is now mature enough to include security planning at the strategic level and not treated as an afterthought or assumption that the IT department or section will take care of it.

All three groups measured agree Information Security is or should be more aligned to the Strategic Information Systems Plan and the Strategic Business Plan.

4.6 Summary

This chapter included information about the preparation of information used in analyzing the data from the survey conducted. Modifications to the data were discussed and an explanation was given for the removal of 6 data points in the original data set. An impressive survey response rate conducted was detailed and referenced so the reader understands the results from the survey were representative. Demographic analysis also showed there was good representation of technicians, middle managers, and senior managers. Hypothesis testing and analysis showed each hypothesis results and a summary was given for each hypothesis. Investigative question were answered at the end of this chapter. The next chapter will include conclusions and recommendations for further action.

The significance of these finding is that all three of the groups (Technicians, Middle Managers, and Senior Managers) within the Marine Corps feel there is alignment between all three model constructs. These findings could explain why the Marine Corps' networks are harder to break into. The findings also suggest all three groups have a

shared fundamental understanding of the constructs. Having this shared understanding better enables the Marine Corps to succeed in implementing all aspects of information assurance.

5 Conclusions and Recommendations

5.1 Chapter Overview

This chapter provides conclusions of the research and recommendations for continuing the research and applying the same methodology across different DoD sectors. The significance of the research is discussed and recommendations for further action are provided.

5.2 Conclusions of Research

This research introduced Information Security (INFOSEC) as the Information Security Plan (ISP) to the existing alignment model construct between Strategic Information System Planning (SISP) and Strategic Business Planning (SBP).

The purpose of this research is an attempt to address a statement made at an OSD sponsored conference: *Marine Corps' networks are harder to break into.* The researcher wanted to ascertain if alignment existed in the relationship between the Strategic Business Plan (SBP), Strategic Information Systems Plan (SISP) and the Information Security Plan (ISP). A research model exists showing the dichotomous relationship between SBP and SISP (Kearns and Lederer 2000). This research extends the Strategic Information Systems Plan (SISP) and Strategic Business Plan (SBP) alignment model construct by including Information Security (INFOSEC) as an additional component considered essential to the success of network centric organizations.

A survey was designed to analyze a public organization (the United States Marine Corps) to determine if this alignment is present. Unlike previous studies that targeted senior leaders such as the CEO, CIO, CISO, and senior managers; this study targets an

information assurance workforce ranging from technicians to senior managers. Six hypotheses were considered to measure the two-way alignment among the three components of the model construct. The survey instrument was tailored for a public sector organization. A vertical, cross-sectional sample from a Department of Defense organization was surveyed (n = 149). The data were analyzed using the Kruskal-Wallis non-parametric test with α=.05.

A Cronbach's alpha test was performed on the questions since many of the questions were not found in previous research to measure reliability. The results from this test conclude that all of the questions measure what they are intended to measure. Additional output of the Cronbach's alpha test is available in Appendix D.

Results indicate that strong alignment exists between SISP - SBP (p = .232 and .910), SISP - ISP (p = .445, and .467), and SBP - ISP (p = .205 and .490). These results also indicate that all three groups agree that alignment exists between all three model constructs. The addition of the Information Security construct to the SBP-SISP model is therefore validated.

5.3 Significance of Research

This research fills a gap in the literature where information security appears to be missing from higher level business policies. The results from this study indicate Information Security (INFOSEC) is present at the strategic planning level. INFOSEC planning should not be thought of as second hand or a part of the SISP. The ISP is a separate planning consideration.

A possible reason the Marine Corps' networks are harder to break into could be

that most personnel within the information assurance workforce have the same understanding of the commander's intent as indicated by the responses from the survey. In addition, having this shared holistic understanding allows personnel to reach the same unified goal of protecting the Global Information Grid (GIG). Combine this shared understanding with increased training and certifications as required with the DoD 8570, the Marine Corps could be in a better position than other branches of the armed services to defend its networks.

The Marine Corps Communications Chiefs play a large part in the defense of the GIG. The relationship between the Communication Chiefs and the Information Assurance workforce are a lot stronger than they were ten years ago. This relationship better enables the whole communication occupational field to work together and allows broader thinking than previously possible.

Certification requirements, continuous training, and education are taking place early in the career path of military personnel. Entry level Marines are given the opportunity to obtain entry level certifications while they are in school before they get to their first command. This ensures the combatant commander that his newest Marines out of Military Occupational School (MOS) are capable of performing their job without additional needing on-the-job training (OJT).

5.4 Recommendations for Future Research

This work should be extended to other public sector organizations to validate the results and consideration of information security as a component to the alignment model. The results of the study should be replicated with other military services, as well as other

public and private organizations to see if information security alignment is a valid component of the proposed model construct. Application of this study towards other organizations should review the survey design and ensure all of the demographic questions are mutually exclusive.

Appendix A: IRB Exemption Letter

December 17, 2009

Dr. Michael Grimaila,

I have reviewed your study entitled "Strategic Security Alignment" and found that your study qualifies for an IRB exemption.

Per 32 CFR 219.101 (b)(2), Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless: (i) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation is exempt.

Your study qualifies for this exemption because the demographic data you are collecting cannot realistically be expected to map a given response to a specific subject, and the questions you are asking could not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation. Finally, while you are collecting names, this is a required and natural consequence of your selected data collection methodology. These names will be protected at all times, only be known to the researchers, and managed according to the AFIT interview protocol.

This determination pertains only to the Federal, DoD, and Air Force regulations that govern the use of human subjects in research. It does not constitute final approval to conduct the study which should be granted by you research advisor. Further, if a subject's future response reasonably places them at risk of criminal or civil liability or is damaging to their financial standing, employability, or reputation, you are required to file an adverse event report with this office immediately.

WILLIAM A. CUNNINGHAM, PhD
AFIT IRB Research Reviewer

Appendix B: Visual Basic Code for determining demographic possibilities

This code was developed and used in Microsoft Visual Basic within Microsoft Office Excel 2007 version (12.0.6524.5003 SP2).

```
Sub combine_columns()
Dim Mos As Variant
Dim Rank As Variant
Dim Years As Variant
Dim Moscount As Integer
Dim rankcount As Integer
Dim Combo As Variant
Dim ComboString As String

'Thanks to Capt Derek Huber and 2ndLt Kyle Stewart at AFIT Feb 23-24 2010.
'Thanks to Robert G. Rodriguez of McAfee for additional help Feb 24-25 2010.

Range("M1").Select 'Change as appropriate
    For Each Mos In Range("B2:B56") 'Change as appropriate
        Moscount = Moscount + 1
        rankcount = 0
        For Each Rank In Range("A2:A26") 'Change as appropriate
            rankcount = rankcount + 1
            For Each Years In Range("C2:C5")
                '######not enlisted######
                If (Moscount < 25) And (rankcount > 6) Then
                   ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '0211
                ElseIf (Moscount = 1) And (rankcount > 5) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '0231
                ElseIf (Moscount = 2) And (rankcount > 5) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '0612
                ElseIf (Moscount = 3) And (rankcount > 2) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '0619
                ElseIf (Moscount = 4) And (rankcount < 3 Or rankcount > 4) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '0621
                ElseIf (Moscount = 5) And (rankcount > 2) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
```

```
                ActiveCell.Offset(1, 0).Select
            '0622
            ElseIf (Moscount = 6) And (rankcount > 2) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0623
            ElseIf (Moscount = 7) And (rankcount > 2) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0627
            ElseIf (Moscount = 8) And (rankcount > 2) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0628
            ElseIf (Moscount = 9) And (rankcount > 2) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0629
            ElseIf (Moscount = 10) And (rankcount < 3 Or rankcount > 4) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0651
            ElseIf (Moscount = 11) And (rankcount > 2) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0659
            ElseIf (Moscount = 12) And (rankcount < 3 Or rankcount > 4) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0681
            ElseIf (Moscount = 13) And (rankcount < 3 Or rankcount > 6) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0689
            ElseIf (Moscount = 14) And (rankcount < 2 Or rankcount > 6) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0699
            ElseIf (Moscount = 15) And (rankcount < 5 Or rankcount > 6) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '2611
            ElseIf (Moscount = 16) And (rankcount > 6) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
```

```
                ActiveCell.Offset(1, 0).Select
            '2621
            ElseIf (Moscount = 17) And (rankcount > 4) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '2629
            ElseIf (Moscount = 18) And (rankcount > 6) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '2631
            ElseIf (Moscount = 19) And (rankcount > 4) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '2821
            ElseIf (Moscount = 20) And (rankcount > 2) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '2823
            ElseIf (Moscount = 21) And (rankcount < 3 Or rankcount > 6) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '2847
            ElseIf (Moscount = 22) And (rankcount > 2) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '2862
            ElseIf (Moscount = 23) And (rankcount < 2 Or rankcount > 4) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '6694
            ElseIf (Moscount = 24) And (rankcount > 6) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select

            '######not officer######
            ElseIf (Moscount > 24 And Moscount < 31) And (rankcount < 7 Or
rankcount > 12) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0602
            ElseIf (Moscount = 25) And (rankcount < 7 Or rankcount > 11) Then
                ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                ActiveCell.Offset(1, 0).Select
            '0603
            ElseIf (Moscount = 26) And (rankcount < 7 Or rankcount > 11) Then
```

```
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '8055
                ElseIf (Moscount = 27) And (rankcount < 7 Or rankcount > 12) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '8846
                ElseIf (Moscount = 28) And (rankcount < 7 Or rankcount > 12) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '8848
                ElseIf (Moscount = 29) And (rankcount < 7 Or rankcount > 12) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '8858
                ElseIf (Moscount = 30) And (rankcount < 7 Or rankcount > 12) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select

                '######not warrant######
                '0610 LDO
                ElseIf (Moscount = 31) And (rankcount < 9 Or rankcount = 12 Or
rankcount > 17) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '0620 LDO
                ElseIf (Moscount = 32) And (rankcount < 9 Or rankcount = 12 Or
rankcount > 17) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                '0650 LDO
                ElseIf (Moscount = 33) And (rankcount < 9 Or rankcount = 12 Or
rankcount > 17) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select

               ' ElseIf (Moscount > 30 And Moscount < 34) And (rankcount < 13 Or
rankcount > 17) Then
                '     ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                '     ActiveCell.Offset(1, 0).Select

                '######not civilian######
                ElseIf (Moscount > 33 And Moscount < 54) And (rankcount < 18 Or
rankcount > 23) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
```

```
                    ActiveCell.Offset(1, 0).Select

                '######not contractor######
                ElseIf (Moscount > 53) And (rankcount < 24) Then
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years and "     Not Valid"
                    ActiveCell.Offset(1, 0).Select
                Else
                    ActiveCell.Formula = Mos and "     " and Rank and "     " and
Years
                    ActiveCell.Offset(1, 0).Select
                End If
            Next
        Next
    Next

    ' Moscount must be initialized to 0
    Moscount = 0
    rankcount = 0
Range("N1").Select 'Change as appropriate
    For Each Mos In Range("B2:B56") 'Change as appropriate
        Moscount = Moscount + 1
        rankcount = 0
        For Each Rank In Range("A2:A26") 'Change as appropriate
            rankcount = rankcount + 1
            For Each Years In Range("C2:C5")

                ' Use the checks from the previous section to determine if the line
is Valid
                '######not enlisted######
                If (Moscount < 25) And (rankcount > 6) Then
                   ActiveCell.Offset(1, 0).Select
                '0211
                ElseIf (Moscount = 1) And (rankcount > 5) Then
                    ActiveCell.Offset(1, 0).Select
                '0231
                ElseIf (Moscount = 2) And (rankcount > 5) Then
                    ActiveCell.Offset(1, 0).Select
                '0612
                ElseIf (Moscount = 3) And (rankcount > 2) Then
                    ActiveCell.Offset(1, 0).Select
                '0619
                ElseIf (Moscount = 4) And (rankcount < 3 Or rankcount > 4) Then
                    ActiveCell.Offset(1, 0).Select
                '0621
                ElseIf (Moscount = 5) And (rankcount > 2) Then
                    ActiveCell.Offset(1, 0).Select
                '0622
                ElseIf (Moscount = 6) And (rankcount > 2) Then
                    ActiveCell.Offset(1, 0).Select
                '0623
                ElseIf (Moscount = 7) And (rankcount > 2) Then
                    ActiveCell.Offset(1, 0).Select
                '0627
                ElseIf (Moscount = 8) And (rankcount > 2) Then
```

```
                ActiveCell.Offset(1, 0).Select
            '0628
            ElseIf (Moscount = 9) And (rankcount > 2) Then
                ActiveCell.Offset(1, 0).Select
            '0629
            ElseIf (Moscount = 10) And (rankcount < 3 Or rankcount > 4) Then
                ActiveCell.Offset(1, 0).Select
            '0651
            ElseIf (Moscount = 11) And (rankcount > 2) Then
                ActiveCell.Offset(1, 0).Select
            '0659
            ElseIf (Moscount = 12) And (rankcount < 3 Or rankcount > 4) Then
                ActiveCell.Offset(1, 0).Select
            '0681
            ElseIf (Moscount = 13) And (rankcount < 3 Or rankcount > 6) Then
                ActiveCell.Offset(1, 0).Select
            '0689
            ElseIf (Moscount = 14) And (rankcount < 2 Or rankcount > 6) Then
                ActiveCell.Offset(1, 0).Select
            '0699
            ElseIf (Moscount = 15) And (rankcount < 5 Or rankcount > 6) Then
                ActiveCell.Offset(1, 0).Select
            '2611
            ElseIf (Moscount = 16) And (rankcount > 6) Then
                ActiveCell.Offset(1, 0).Select
            '2621
            ElseIf (Moscount = 17) And (rankcount > 4) Then
                ActiveCell.Offset(1, 0).Select
            '2629
            ElseIf (Moscount = 18) And (rankcount > 6) Then
                ActiveCell.Offset(1, 0).Select
            '2631
            ElseIf (Moscount = 19) And (rankcount > 4) Then
                ActiveCell.Offset(1, 0).Select
            '2821
            ElseIf (Moscount = 20) And (rankcount > 2) Then
                ActiveCell.Offset(1, 0).Select
            '2823
            ElseIf (Moscount = 21) And (rankcount < 3 Or rankcount > 6) Then
                ActiveCell.Offset(1, 0).Select
            '2847
            ElseIf (Moscount = 22) And (rankcount > 2) Then
                ActiveCell.Offset(1, 0).Select
            '2862
            ElseIf (Moscount = 23) And (rankcount < 2 Or rankcount > 4) Then
                ActiveCell.Offset(1, 0).Select
            '6694
            ElseIf (Moscount = 24) And (rankcount > 6) Then
                ActiveCell.Offset(1, 0).Select

            '######not officer######
            ElseIf (Moscount > 24 And Moscount < 31) And (rankcount < 7 Or
rankcount > 12) Then
                ActiveCell.Offset(1, 0).Select
            '0602
```

```
                ElseIf (Moscount = 25) And (rankcount < 7 Or rankcount > 11) Then
                    ActiveCell.Offset(1, 0).Select
                '0603
                ElseIf (Moscount = 26) And (rankcount < 7 Or rankcount > 11) Then
                    ActiveCell.Offset(1, 0).Select
                '8055
                ElseIf (Moscount = 27) And (rankcount < 7 Or rankcount > 12) Then
                    ActiveCell.Offset(1, 0).Select
                '8846
                ElseIf (Moscount = 28) And (rankcount < 7 Or rankcount > 12) Then
                    ActiveCell.Offset(1, 0).Select
                '8848
                ElseIf (Moscount = 29) And (rankcount < 7 Or rankcount > 12) Then
                    ActiveCell.Offset(1, 0).Select
                '8858
                ElseIf (Moscount = 30) And (rankcount < 7 Or rankcount > 12) Then
                    ActiveCell.Offset(1, 0).Select

                '######not warrant######
                '0610 LDO
                ElseIf (Moscount = 31) And (rankcount < 9 Or rankcount = 12 Or
rankcount > 17) Then
                    ActiveCell.Offset(1, 0).Select
                '0620 LDO
                ElseIf (Moscount = 32) And (rankcount < 9 Or rankcount = 12 Or
rankcount > 17) Then
                    ActiveCell.Offset(1, 0).Select
                '0650 LDO
                ElseIf (Moscount = 33) And (rankcount < 9 Or rankcount = 12 Or
rankcount > 17) Then
                    ActiveCell.Offset(1, 0).Select

                'ElseIf (Moscount > 30 And Moscount < 34) And (rankcount < 13 Or
rankcount > 17) Then
                '    ActiveCell.Offset(1, 0).Select

                '######not civilian######
                ElseIf (Moscount > 33 And Moscount < 54) And (rankcount < 18 Or
rankcount > 23) Then
                    ActiveCell.Offset(1, 0).Select

                '######not contractor######
                ElseIf (Moscount > 53) And (rankcount < 24) Then
                    ActiveCell.Offset(1, 0).Select

                ' If we made it this far, then the line must be valid
                ' think of the following code as fitting inside the else statement
                ' of the previous section

                'Start Technician
                ElseIf (StrComp(Rank, "Cpl or below", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Technician"
                    ActiveCell.Offset(1, 0).Select

                ElseIf (StrComp(Rank, "Sgt", vbTextCompare) = 0) Then
```

```
    ActiveCell.Offset.Value = "Technician"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "SSgt", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Technician"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "GS-5 or below", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Technician"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "GS-6 or GS-7", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Technician"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "Contractor", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Technician"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "Foreign-National", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Technician"
    ActiveCell.Offset(1, 0).Select

'Start Middle Manager
ElseIf (StrComp(Rank, "GySgt", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Middle Manager"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "MSgt", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Middle Manager"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "WO1", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Middle Manager"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "CWO2", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Middle Manager"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "CWO3", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Middle Manager"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "GS-8 or GS-9", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Middle Manager"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "GS-10 or GS-11", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Middle Manager"
    ActiveCell.Offset(1, 0).Select

ElseIf (StrComp(Rank, "2ndLt", vbTextCompare) = 0) Then
    ActiveCell.Offset.Value = "Technician"
    ActiveCell.Offset(1, 0).Select
```

```
                ElseIf (StrComp(Rank, "1stLt", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Middle Manager"
                    ActiveCell.Offset(1, 0).Select

                'Start Senior Manager
                ElseIf (StrComp(Rank, "MGySgt", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Senior Manager"
                    ActiveCell.Offset(1, 0).Select

                ElseIf (StrComp(Rank, "CWO4", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Senior Manager"
                    ActiveCell.Offset(1, 0).Select

                ElseIf (StrComp(Rank, "CWO5", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Senior Manager"
                    ActiveCell.Offset(1, 0).Select

                ElseIf (StrComp(Rank, "Capt", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Senior Manager"
                    ActiveCell.Offset(1, 0).Select

                ElseIf (StrComp(Rank, "Maj", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Senior Manager"
                    ActiveCell.Offset(1, 0).Select

                ElseIf (StrComp(Rank, "LtCol", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Senior Manager"
                    ActiveCell.Offset(1, 0).Select

                ElseIf (StrComp(Rank, "Col", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Senior Manager"
                    ActiveCell.Offset(1, 0).Select

                ElseIf (StrComp(Rank, "GS-12 or GS-13", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Senior Manager"
                    ActiveCell.Offset(1, 0).Select

                ElseIf (StrComp(Rank, "GS-14 or GS-15", vbTextCompare) = 0) Then
                    ActiveCell.Offset.Value = "Senior Manager"
                    ActiveCell.Offset(1, 0).Select
                Else
                    ActiveCell.Offset(1, 0).Select
                End If
            Next
        Next
    Next

End Sub
```

Appendix C: C Program code for determining valid versus non valid responses.

```
      // ParseSurvey.cpp : Parse Scanlan Survey and sort into usable
and unusable
      // Author: John Scanlan and Michael R. Grimaila
      // Last Updated:   27 April 2010
      //

      #include "stdafx.h"
      #include <stdio.h>
      #include <conio.h>
      #include <string.h>
      #include <stdlib.h>
      #include <time.h>

      FILE *validsfile;
      FILE *infile;
      FILE *techfile;
      FILE *midfile;
      FILE *seniorfile;
      FILE *badfile;
      FILE *debugfile;
      FILE *allfile;

      int _tmain(int argc, _TCHAR* argv[])
      {
         int linesread;
         char line[5000];
         char curline[5000];
         char chopline[5000];
         char validlist[1900][200];
         char validtype[1900];
         char Check[200];
         char Check2[200];
         char seps[] = ",\t\n";
         int Len;
         int MaxLen;
         int tech;
         int mid;
         int senior;
         int bad;
         int found;
         int numvalid;
         int numtypes;
         int fix;
         int fixrank;
         int checkit;
         int checkitfound;
         char *tok;
         int tokens;
         int maxtokens;
         int positionindex;
         char findstart[] = "Log format:";
```

```
        char validsfilename[] =
"C:\\AFIT\\Scanlan\\ParseSurvey\\Debug\\valids3.csv";
        char typesfilename[] =
"C:\\AFIT\\Scanlan\\ParseSurvey\\Debug\\types3.csv";
        char infilename[] =
"C:\\AFIT\\Scanlan\\ParseSurvey\\Debug\\data.csv";
        char techfilename[] =
"C:\\AFIT\\Scanlan\\ParseSurvey\\Debug\\techgood.csv";
        char midfilename[] =
"C:\\AFIT\\Scanlan\\ParseSurvey\\Debug\\midgood.csv";
        char seniorfilename[] =
"C:\\AFIT\\Scanlan\\ParseSurvey\\Debug\\seniorgood.csv";
        char badfilename[] =
"C:\\AFIT\\Scanlan\\ParseSurvey\\Debug\\bad.csv";
        char debugfilename[] =
"C:\\AFIT\\Scanlan\\ParseSurvey\\Debug\\debug.dat";
        char allfilename[] =
"C:\\AFIT\\Scanlan\\ParseSurvey\\Debug\\all.dat";
        char tenplus[] = "10 + Years";
        char slt[] = "2ndLt (O3E)";
        char flt[] = "1stLt (O3E)";
        char cap[] = "Capt (O3E)";
        int i;
        int j;
        char LineTokens[100][100];
        int done;
        int val;

        /* clear valids array */
        for(i=0; i<1900; i++)
        {
              validtype[i] = 0;
            for(j=0; j<200; j++)
              {
               validlist[i][j]=0;
              }
        }

        /* read in valids */
        validsfile = fopen (validsfilename, "rt");
        numvalid = 0;
        MaxLen = 0;
        while(fgets(line, 5000, validsfile) != NULL)
        {
           for(i=0; (i<200) andand (line[i]!=0x0A); i++)
             {
              validlist[numvalid][i]=line[i];
             }
           validlist[numvalid][i]=0x00;
             Len = (int) strlen(validlist[numvalid]);
             if(Len > MaxLen)
             {
                   MaxLen = Len;
             }
             numvalid++;
```

```
        }
        fclose(validsfile);
        printf("Processed %d valid type entries\n",numvalid);
        /*printf("Maximum length: %d\n",MaxLen);*/

        /* read in types */
        numtypes=0;
        validsfile = fopen (typesfilename, "rt");
        while(fgets(line, 5000, validsfile) != NULL)
        {
           switch(line[0])
             {
                case 0x53:
                        /* Senior Manager */
                        validtype[numtypes++] = 1;
                      break;

                case 0x4D:
                        /* Middle Manager */
                        validtype[numtypes++] = 2;
                      break;

                case 0x54:
                        /* Technician */
                        validtype[numtypes++] = 3;
                      break;

                  default:
                        printf("Major Error! Exiting on type number
%d\n",numtypes);
                        fclose(validsfile);
                        exit(1);
                      break;
             }
        }
        fclose(validsfile);
        printf("Processed %d type entries\n",numtypes);


        /* 11 9 3 */

        /* open data files */
        infile = fopen (infilename, "rt");
        techfile = fopen (techfilename, "wt");
        midfile = fopen (midfilename, "wt");
        seniorfile = fopen (seniorfilename, "wt");
        badfile = fopen (badfilename, "wt");
        debugfile = fopen (debugfilename, "wt");
        allfile = fopen (allfilename, "wt");

        linesread = 0;
        maxtokens = 0;

        found = 0;
        /* skip one line */
```

```
         fgets(line, 5000, infile);

         if(ferror(infile))
         {
            /* file I/O error has occurred, so abort */
              fprintf(stderr, "\nRead error occurred on access to file:
%s\n", infilename);
            fclose(infile);
            fclose(techfile);
              fclose(midfile);
              fclose(seniorfile);
            fclose(badfile);
              fclose(debugfile);
              fclose(allfile);
              exit(1);
         }

         done = 0;
         tech = 0;
         mid = 0;
         senior = 0;
         bad = 0;
         while( (fgets(line, 5000, infile) != NULL) andand (!done) )
         {
            strncpy(curline,line,5000);
              strncpy(chopline,line,5000);
            Len = (int)strlen(chopline);
              chopline[Len]=0x00;
              chopline[Len-1]=0x00;

            tokens = 0;

              /* clear out stored tokens */
              for(i=0; i<100; i++)
              {
                 for(j=0; j<100; j++)
                 {
                  LineTokens[i][j]=(char)0;
                   }
              }

            /* get length of line */
            Len = (int)strlen(line);

              if(Len < 10)
              {
               /* end of data lines, so done processing */
                     done = 1;
              }
              else
              {
               tok = strtok(line, seps);
                 while( (tok != NULL) andand (tokens < 50) )
                 {
                        tokens++;
```

```
                        /* While there are tokens in "string" */
                        /* fprintf(outfile,"%s,", tok);*/
                        sprintf(LineTokens[tokens-1],"%s", tok);
                        /* fprintf(stderr,"token[%d]=%s,",tokens,tok);
*/
                        /* Get next token: */
                        tok = strtok(NULL, seps);
                }
                    /* fprintf(outfile,"\n"); */
                    if(tokens>maxtokens)
                    {
                       maxtokens = tokens;
                    }
                    /* increment line counter */
                  linesread++;
               }
               /* fprintf(outfile,"%d\n,", Len);  debug to see how many
characters are in the line */
               if(!done)
               {
                  /* valid line needs to be processed */

                  /* dump tokens */
                    fprintf(debugfile,"\n");
                  for(i=0; i<tokens; i++)
                  {

fprintf(debugfile,"Line[%d]Token[%d]=%s\n",linesread,i,LineTokens[i]);
                  }
               }
               /*  9 J - MIL Rank     X    N/A   N/A
                  10 K - CIV Rank    N/A   X     Other
                    11 L - Other                  X

                12 M - MOS          Y    N/A   N/A    Other
                    13 N - Class       N/A   Y     Other  N/A
                    14 O - Other                   Y      Y

                    MIL MOS          9 11
                    MIL OTHER        9 13
                    CIV RANK CLASS  10 12
                    CIV RANK OTHER  10 13
                    CIV OTHER CLASS 11 13
                    CIV OTHER OTHER 11 14
                    N = 0x4E
                    O = 0x4F
              */
               checkit = 0;
               checkitfound = 0;
             fix = 0;
               if(!strcmp(tenplus,LineTokens[5]))
               {
                  /* found a 10 + */
                fix=1;
               }
```

```
                /* Determine rank and job code */
                /* mil or civ or civ/other */
                if(LineTokens[9][0] != 0x4E)
                {
                 /* miltary */
                 /* fix
                          2ndLt = 2ndLt (O3E)
                          1stLt = 1stLt (O3E)
                          Capt = Capt (O3E)
                    */
                fixrank = 0;
                  if(!strcmp(slt,LineTokens[9]))
                  {
                      /* found a 2ndLt (O3E) */
                    fixrank=1;
                          LineTokens[9][5]=0x00;
                  }
                    else
                    {
                     if(!strcmp(flt,LineTokens[9]))
                     {
                         /* found a 1stLt (O3E) */
                       fixrank=2;
                             LineTokens[9][5]=0x00;
                     }
                       else
                       {
                          if(!strcmp(cap,LineTokens[9]))
                           {
                             /* found a Capt (O3E) */
                          fixrank=3;
                                  LineTokens[9][4]=0x00;
                           }
                       }
                    }

                 /* now get job code */
                 if(LineTokens[11][0] == 0x4F)
                     {
                           /* MOS other */
                           checkit=1;
                           val = (int) atoi(LineTokens[13]);

                           if(fix)
                           {
                              sprintf(Check,"%s     %s     10+
Years",LineTokens[13],LineTokens[9]);
                           }
                           else
                           {
                              sprintf(Check,"%s     %s
%s",LineTokens[13],LineTokens[9],LineTokens[5]);
                           }
```

```
                        if(fix)
                        {
                           sprintf(Check2,"%04d     %s     10+
Years",val,LineTokens[9]);
                        }
                        else
                        {
                           sprintf(Check2,"%04d     %s
%s",val,LineTokens[9],LineTokens[5]);
                        }
                    }
                    else
                    {
                          /* known MOS */
                    val = (int) atoi(LineTokens[11]);
                          if(fix)
                          {
                           sprintf(Check,"%04d     %s     10+
Years",val,LineTokens[9]);
                          }
                          else
                          {
                                sprintf(Check,"%04d     %s
%s",val,LineTokens[9],LineTokens[5]);
                          }
                    }
               }
               else
               {
                /* civilian */
                /* now get rank */
                if(LineTokens[10][0] == 0x4F)
                    {
                          /* other rank */
                    if(LineTokens[13][0] == 0x4F)
                        {
                                /* other job */
                                if(fix)
                                {
                                   sprintf(Check,"%s     %s     10+
Years",LineTokens[14],LineTokens[11]);
                                }
                                else
                                {
                                      sprintf(Check,"%s     %s
%s",LineTokens[14],LineTokens[11],LineTokens[5]);
                                }
                          }
                          else
                       {
                                /* job */
                                if(fix)
                                {
                                   sprintf(Check,"%s     %s     10+
Years",LineTokens[13],LineTokens[11]);
```

```
                                    }
                                    else
                                    {
                                          sprintf(Check,"%s     %s
%s",LineTokens[13],LineTokens[11],LineTokens[5]);
                                    }
                              }
                        }
                        else
                        {
                              /* known rank */
                        if(LineTokens[13][0] == 0x4E)
                            {
                                    /* other job */
                                    if(fix)
                                    {
                                       sprintf(Check,"%s     %s     10+
Years",LineTokens[13],LineTokens[10]);
                                    }
                                    else
                                    {
                                          sprintf(Check,"%s     %s
%s",LineTokens[13],LineTokens[10],LineTokens[5]);
                                    }
                              }
                              else
                           {
                                    /* job */
                                    if(fix)
                                    {
                                       sprintf(Check,"%s     %s     10+
Years",LineTokens[12],LineTokens[10]);
                                    }
                                    else
                                    {
                                          sprintf(Check,"%s     %s
%s",LineTokens[12],LineTokens[10],LineTokens[5]);
                                    }
                              }
                        }
                  }

                  /* printf("Line: %d Check: %s\n",linesread,Check); */

                  found = 0;
                  for(i=0; (i<numvalid) andand (!found); i++)
                  {
                        if(!strcmp(Check,validlist[i]))
                        {
                              found = i;
                        }
                        if(checkit)
                        {
                         if(!strcmp(Check2,validlist[i]))
                           {
```

```
                        found = i;
                          checkitfound = 1;
                     }
                  }
            }

            if(found)
            {
                 positionindex=0;
                 switch(validtype[found])
               {
                  case 1:
                       /* Senior Manager */
                       fprintf(seniorfile,"%s",curline);
                       senior++;
                       positionindex=1;
                     break;

                  case 2:
                       /* Middle Manager */
                 fprintf(midfile,"%s",curline);
                       mid++;
                       positionindex=2;
                     break;

                  case 3:
                       /* Technician */
                 fprintf(techfile,"%s",curline);
                       tech++;
                       positionindex=3;
                     break;

                 default:
                       printf("Major Error! Exiting on %s number
%d\n",curline,found);
                       fclose(validsfile);
                       exit(1);
                     break;
               }
                 if(checkitfound)
                 {
                       printf("LINE: %3d VALID:   %s INDEX:
%i\n",linesread,Check2,found);
                 }
                 else
                 {
                    printf("LINE: %3d VALID:   %s INDEX:
%i\n",linesread,Check,found);
                 }
                 fprintf(allfile,"%s,%d\n",chopline,positionindex);
            }
            else
            {
                  fprintf(badfile,"%s NOT VALID %d\n",Check,found);
              fprintf(badfile,"%s",curline);
```

```
                    bad++;
                    if(checkit)
                    {
                          printf("LINE: %3d INVALID: Other MOS so tried
both %s and %s\n",linesread,Check,Check2);
                    }
                    else
                    {
                          printf("LINE: %3d INVALID:
%s\n",linesread,Check);
                    }
                    fprintf(allfile,"%s,X\n",chopline);
               }
          }

          printf ("ParseSurvey processed %d lines. Senior = %d Mid = %d
Tech = %d Bad = %d", linesread,senior,mid,tech,bad);

          fclose(infile);
          fclose(techfile);
          fclose(midfile);
          fclose(seniorfile);
          fclose(badfile);
          fclose(debugfile);
          fclose(allfile);

          return 0;
}
```

EOF (not included in file)

==========

Associated H file for the C program to parse valid responses.

```
// stdafx.h : include file for standard system include files,
// or project specific include files that are used frequently,but
// are changed infrequently
//

#pragma once


#include <iostream>
#include <tchar.h>
```

// TODO: reference additional headers your program requires here

Appendix D: Cronbach’s alpha of each hypothesis question set.

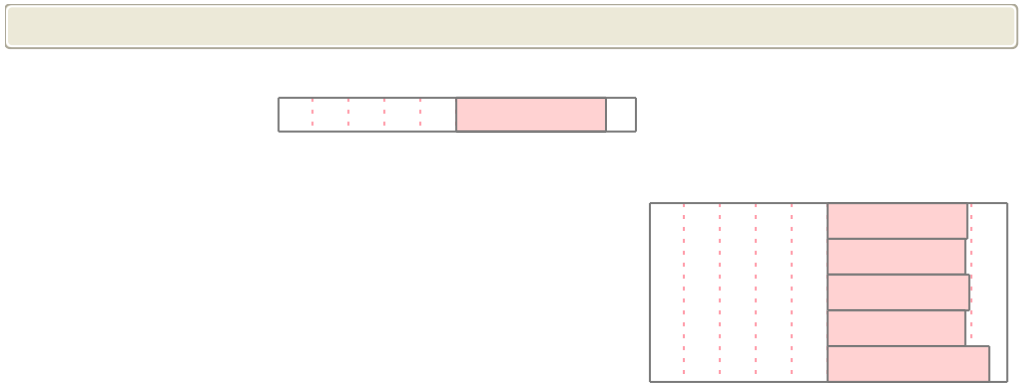

Figure 36: Cronbach's Alpha of H1a

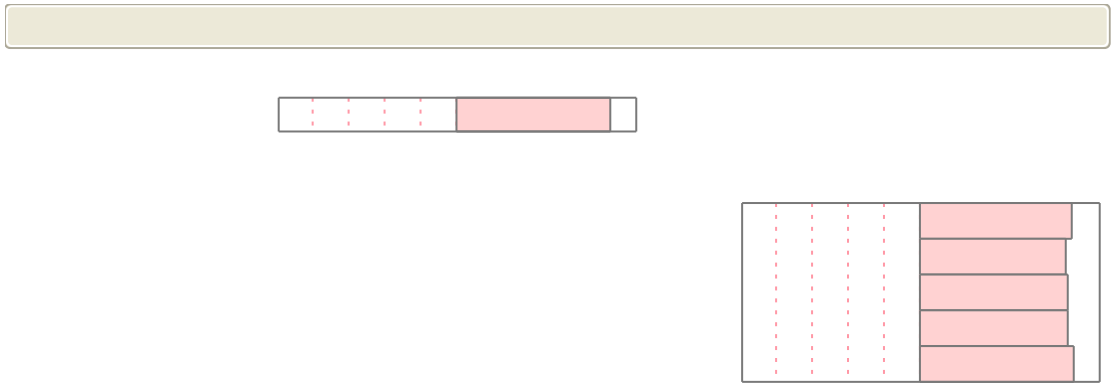

Figure 37: Cronbach's Alpha of H1b

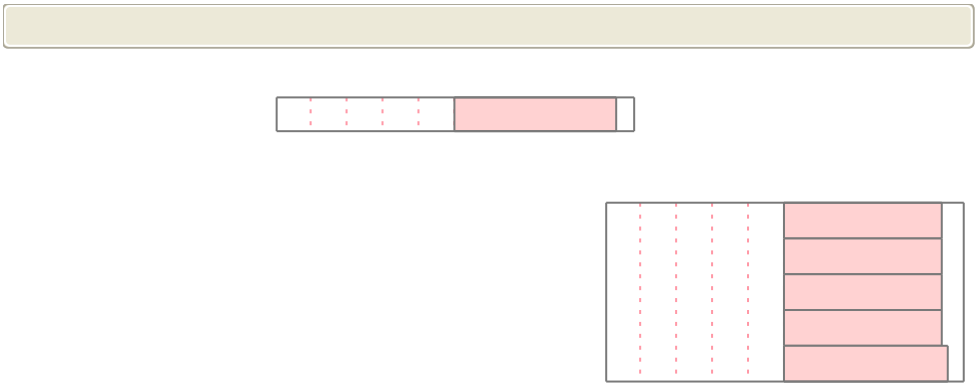

Figure 38: Cronbach's Alpha of H2a

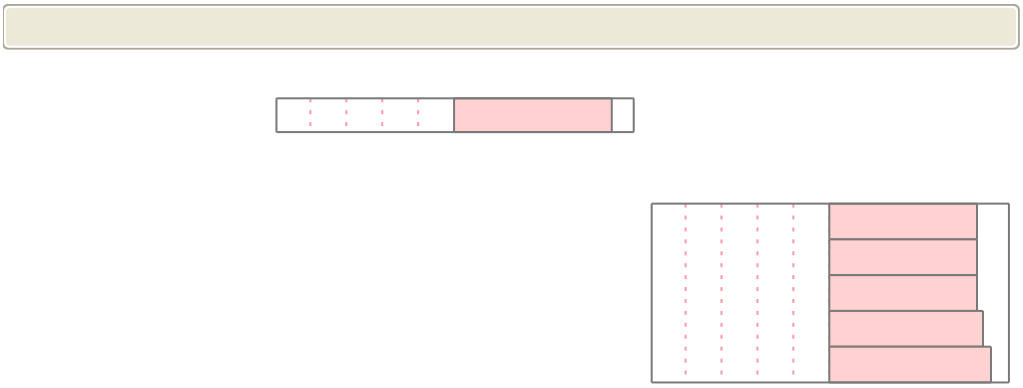

Figure 39: Cronbach's Alpha of H2b

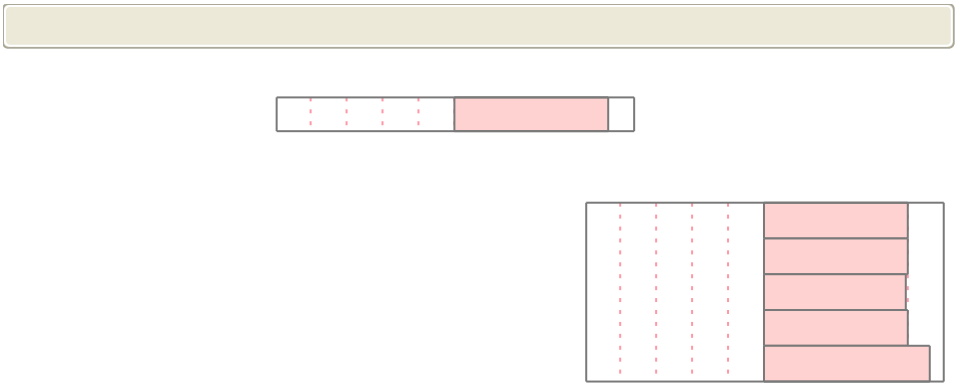

Figure 40: Cronbach's Alpha of H3a

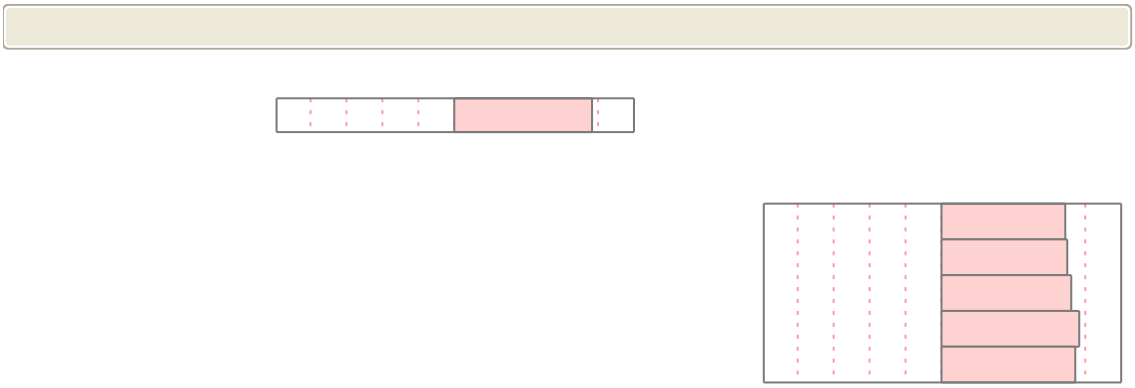

Figure 41: Cronbach's Alpha of H3b

Appendix E: Alignment Survey

Strategic Security alignment

The purpose of this survey is to assess the alignment between the Information Security Program/Plan, the Communication Plan, and the Operation Plan. This research is predicated upon the following research question:

Has the paradigm of strategic planning alignment changed sufficiently to support the new role of Information Security?

Demographics:

How long have you worked in your current Information Assurance or Network Security billet?	0-3 years	3-7 years	7-10 years	10+ years
What is your highest level of formal education completed?	High School	Undergraduate	Graduate	Post-Graduate
How many years of experience do you have in Information Assurance or Network Security?	0-3 years	3-7 years	7-10 years	10+ years
What is your DoD 8570 IAT billet level?	N/A	IAT level I	IAT level II	IAT level III
What is your DoD 8570 IAM billet level?	N/A	IAM level I	IAM level II	IAM level III
What is your current organization level?	Company	Group/Battalion	Base/Wing/MSC	MEF/Higher HQ
What is your current rank?	Cpl or below Sgt SSgt GySgt MSgt MGySgt 2ndLt 2ndLt (O1E)	Capt Capt (O3E) Maj LtCol Col GS-5 or below GS-6 or GS-7 GS-8 or GS-9	GS-12 or GS-13 GS-14 or GS-15 WO1 CWO2 CWO3 CWO4 CWO5	Contractor Foreign-National Other

	1stLt 1stLt (O2E)	GS-10 or GS-11		
What is your primary MOS/Civilian Classification?	Military 0211 0231 0602 0603 0610 0612 0619 0620 0621 0622 0623 0627 0628 0629 0650	0651 0689 0699 2611 2621 2629 2631 2821 2823 2847 2862 6694 8055 8846 8848 8858	Civilian 0332 0334 0335 0340 0343 0390 0391 0392 0854 0855 0856 1410 1411 1421 1550	2203 2204 2210 N/A Other
What would best describe your civilian equivalent billet?				
Chief Executive Officer (CEO) Chief Information Officer (CIO) Chief Information Security Officer (CISO) Chief Operations Officer (COO) Chief Technology Officer (CTO) Computer Data Entry Operator Computer Data Entry Supervisor Computer Help Desk Supervisor Computer Help Desk Support		Computer Operations Supervisor Computer Security Analyst Computer Security Coordinator Computer Security Engineer Computer Security Specialist Computer Systems and Program Director Data Security Analyst Network Communications Technician Network Engineer		

Computer Operations Director Computer Operations Manager		Network/Data Communications Manager Webmaster Other

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Communication Plan alignment with the Operation Plan					
The COMPLAN reflects the mission statement.	1	2	3	4	5
The COMPLAN reflects the mission goals.	1	2	3	4	5
The COMPLAN has language referencing the OPLAN.	1	2	3	4	5
The COMPLAN supports the strategies of the OPLAN.	1	2	3	4	5
Information Assurance or Network Security personnel are involved in overall communication planning. (not limited to the network security / IA sections)	1	2	3	4	5
Operation Plan alignment with the Communication Plan					
The OPLAN refers to the COMPLAN.	1	2	3	4	5
The OPLAN refers to specific information systems.	1	2	3	4	5
The OPLAN refers to specific information technology.	1	2	3	4	5
The OPLAN has information security language.	1	2	3	4	5
Operational planners (J3, G3, S3) are involved in developing the COMPLAN.	1	2	3	4	5
Communication Plan alignment with the Information Security Plan/Program					
The COMPLAN has language referencing security.	1	2	3	4	5
The COMPLAN has a section devoted to Information Assurance and/or Network Security.	1	2	3	4	5
Information Assurance and/or Network Security personnel	1	2	3	4	5

are involved in planning the COMPLAN.					
The COMPLAN references Information Assurance and/or Network Security policies.	1	2	3	4	5
Information Assurance and/or Network Security are an important part of the COMPLAN planning process.	1	2	3	4	5
Information Security Plan/Program alignment with the Communications Plan					
The Information Security Plan/Program has language referencing the COMPLAN.	1	2	3	4	5
The Information Security Plan/Program references the COMPLAN.	1	2	3	4	5
The Information Security Plan/Program is developed within the scope of the COMPLAN.	1	2	3	4	5
Each system listed in the COMPLAN is listed in the Information Security Plan/Program.	1	2	3	4	5
Information Assurance and/or Network Security is considered an important part of the COMPLAN.	1	2	3	4	5
Operation Plan alignment with the Information Security Plan/Program					
The OPLAN references the Information Security Plan/Program.	1	2	3	4	5
The OPLAN has language about Information Assurance and/or Network Security.	1	2	3	4	5
Information Assurance/Network Security professionals are involved in developing the OPLAN.	1	2	3	4	5
Information Assurance/Network Security is considered a high priority when developing the OPLAN.	1	2	3	4	5
Customers (the warfighter/end user) are involved in operation planning.	1	2	3	4	5

Information Security Plan/Program alignment with the Operation Plan					
The Information Security Plan/Program has language referencing the OPLAN.	1	2	3	4	5
The Information Security Plan/Program supports the mission objectives.	1	2	3	4	5
The Information Security Plan/Program is developed with personnel from J3, G3, or S3.	1	2	3	4	5
Customers (the warfighter/end user) are involved in developing the Information Security Program/Plan.	1	2	3	4	5
Information Assurance/Network Security is considered a high priority when developing the Information Security Plan/Program.	1	2	3	4	5
Additional Comments:					

6 Bibliography

Anderson, Fatima Ferza, and Hugh M Shane. "The impact of netcentricty on virtual teams: the new challenge,." *Team Performance Management: An International Journal*, 2002: 5-12.

Avison, David, Jill Jones, Philip Powell, and David Wilson. "Using and validating the strategic alignment model." *Journal of Strategic Information Systems*, 2004: 223-246.

Baets, Walter. "Aligning information systems with business strategy." *Journal of Strategic Information Systems*, 1992: 205-213.

Barlette, Yves, and Vladislav V Fomin. "Exploring the suitability of IS security management standards for SMEs." *Hawaii International Conference on Systems Sciences.* 2008. 1-10.

Bartlett, James E, Joe W Kotrlik, and Chadwick C Higgins. "Organizational Research: Determining Appropriate Sample Size in Survey Survey Research." *Information Technology, Learning, and Performance Journal*, 2001: 43-50.

Bergeron, Francois, Louis Raymond, and Suzanne Rivard. "Ideal Patterns of Strategic Alignment and Business Performance." *Information & Management*, 2004: 1003-1020.

Boehmer, Wolfgang. "Appraisal of the effectivness and efficiency of an Information Security Management System based on ISO 27001." *International Conference on Emerging Security Information, Systems and Technologies.* IEEE, 2008. 224-231.

Brown, Irwin. "Investigating the Impact of the External Environment on Strategic Information Systems Planning: A Qualitative Inquiry." *SAICSIT*. Wilderness, South Africa: ACM, 2008. 8-15.

Brown, Irwin. "Testing and Extending Theory in Strategic Information Systems Planning Through Literature Analysis." *Information Resources Management Journal*, 2004: 20-48.

Burn, Janice M, and Colonel Szeto. "A comparison of the views of business and IT management on success factors for strategic alignment." *Information & Management*, 2000: 197-216.

Chan, Yolande E, and Sid L Huff. "Strategic Information Systems Alignment." *Business Quarterly*, 1993: 51-55.

CNSSI No. 4009, Committee on National Security Systems. *National Information Assurance (IA) Glossary.* Committee on National Security Systems, 2010.

Cochran, W G. *Sampling techniques (3rd ed.).* New York: Wiley, 1977.

Congressional Budget Office. "Issues Associated with the Global Information Grid Bandwidth Expansion." 2005.

Corder, Gregory W, and Dale I Foreman. *Nonparametric Statistics for Non-Statisticians.* New Jersey: John Wiley & Sons, Inc., 2009.

Croteau, A M, and F Bergeron. "An information technology trilogy: business strategy, technological deployment and oganizational performance." *Journal of Strategic Information Systems*, 2001: 77-99.

Danchev, Dancho. *Building and Implementing a Successful Information Security Policy.* 2003. http://www.windowsecurity.com/pages/security-policy.pdf (accessed 21 October, 2009).

Department of Defense. *Depatment of Defense NetOps Strategic Vision.* The Pentagon - Washington, D.C.: Department of Defense Chief Information Officer, 2008.

Department of Defense. *DoD Net-Centric Data Strategy.* The Pentagon - Washington, D.C.: Department of Defense, 2003.

Department of Defense. "Fiscal Year (FY) 2009 IT President's Budget Request." 2008.

Department of Defense. "Quadrennial Defense Review Report." 2006.

Department of Defense. "Quadrennial Defense Review Report." 2001.

Depatment of Defense. *DoDD 8320.02: Data Sharing in a Net-Centric Depatment of Defense.* ASD(NII)/DOD CIO, 2004.

DoD 8570.1M: Information Assurance Workforce Improvement Program. *DoD 8570.1M: Information Assurance Workforce Improvement Program.* Department of Defense, 2008.

Doherty, N F, C G Marples, and A Suhaimi. "The relative success of alternative approaches to strategic information systems planning: an empirical analysis." *Journal of Strategic Information Systems*, 1999: 263-283.

Doherty, Neil F, and Heather Fulford. "Aligning the information security policy with the strategic information systems plan." *Computers & Security*, 2006: 55-63.

Doherty, Neil F, C G Marples, and A Suhaimi. "The relative success of alternative approaches to strategic information systems planning: an emporocal analysis." *Journal of Strategic Information Systems*, 1999: 263-283.

Duffy, Tim. *Military Experience and CEO's -- Is There a Link.* Korn/Ferry International, 2006.

Flynn, Donal J, and Eva Goleniewska. "A Survey of the use of Strategic Information Systems Planning Approaches in UK Organizations." *Journal of Strategic Information Systems*, 1993: 292-315.

Gay, L R. *Educational Research: Compentencies for analysis and application.* 8th. Upper Saddle River, NJ: Merrill/Prentice Hall, 2005.

Gliem, Joseph A, and Rosemary R Gliem. "Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales." *Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.* Columbus, 2003. 82-88.

Gottschalk, Petter. "Implementing predictors of strategic information systems plans." *Information & Management*, 1999: 77-91.

Grimaila, Michael R, Associate Professor of Information Resource Management, Department of Systems Engineering and Management, Air Force Institute of Technology, Wright-Patterson AFB OH, Personal Interview June 2009.

Hamilton, Michael Braun. *Online Survey Response Rates and Times, Background and Guidence for Industry.* Ipathia, Inc., 2009.

Hartono, Edward, Albert L Lederer, Vijay Sethi, and Youlong Zhuang. "Key Predictors of The Implementation of Strategic Information Systems Plans." *The DATA BASE for Advances in Information Systems*, 2003: 41-53.

Headquarters Marine Corps. *Demographics Update.* Marine Corps Community Services, 2008.

Henderson, J C, and N Venkatraman. "Strategic alignment: Leveraging technology for transforming organizations." *IBM Systems Journal*, 1993: 4-16.

Hevner, Alan R, and James Studnicki. "Strategic Information Systems Planning with Box Structures." *33rd Hawaii International Conference on Systems Sciences.* IEEE, 2000. 1-11.

Higgins, James J. *Introduction to Modern Nonparametric Statistics.* Pacific Grove, CA: Brooks/Cole - Thompson Leanring, 2004.

Hinde, Stephen. *Security surveys spring crop.* Elsevier Science Ltd, 2002.

Hone, Karin, and J H. P. Eloff. *Information security policy - what do international information security standards say?* Elsevier Science Ltd, 2002.

Iacovou, Charalambos L. "The IPACS project: when IT hits the fan." *Journal of Information Technology*, 1999: 267-275.

ISO/IEC 17799. *Information technology - Security techniques - Code of practice for information security management* . ISO, 2005.

IT Governance Institute. "Unlocking Value: An Executive Primer on the Critical Role of IT Governance." 2008.

Kearns, G S, and A L Lederer. "The effect of strategic alignment on the use of IS-based resources for competitive advantage." *Journal of Strategic Information Systems*, 2000: 265-293.

Kearns, Grover S, and Albert L Lederer. "The Influence of Environmental Uncertainty on the Strategic Use of Information Systems." *ACM SIGCPR Computer Personnel*, 1999: 40-68.

King, William R. "How effective is your Information Systems Planning?" *Long Range Planning*, 1988: 103-112.

King, William R. "Strategic Planning for Management Information Systems." *MIS Quarterly*, 1978: 27-37.

Krejcie, R. V., and D. W. Morgan. "Determining sample size for research activities." *Educational and Physchological Measurement*, 1970: 607-610.

Lederer, Albert L, and Hannu Salmela. "Toward a theory of strategic information systems planning." *Journal of Strategic Information Systems*, 1996: 237-253.

Lederer, Albert L, and Veronica Gardiner. "The Process of Strategic Information Planning." *Journal of Strategic Information Systems*, 1992: 76-83.

Lederer, Albert L, and Vijay Sethi. "The Implementation of Strategic Information Systems Planning Methodologies." *MIS Quarterly*, 1988: 445-461.

Lindstrom, John, Soren Samuelsson, Dan Harnesk, and Ann Hagerfors. "The need for imporved alignment between actability, strategic planning of IS and information security." 2000.

Marine Corps Doctrinal Publication 5. "Planning." 1997.

Marine Corps Order P1040.31J, DoD. *Marine Corps Order P1040.31J - Enlisted Retention and Career Development Manual.* DoD, 2004.

Masa'deh, Ra'ed, Ziad Hunaiti, and Ahmad Ali Bani Yaseen. "An integrative Model Linking IT-Business Strategic Alignment and Firm Performance Innovation and Knowledge Management Strategies." *Comminucations of the IBIMA*, 2008: 180-187.

McClave, James T, P George Benson, and Terry Sincich. *Statistics for Business and Economics 10e.* Upper Sadle River, NJ: Pearson Prentice Hall, 2008.

Mentzas, Gregory. "Implementing an IS Strategy - A Team Approach." *Long Range Planning*, 1997: 84-95.

Motjolopane, Ignitia, and Irwin Brown. "Strategic Business-IT Alignment, and Factors of Influence: A Case Study in a Public Tertiary Education Institution." *SAICSIT*. 2004. 147-156.

Mullen, Stanley A. *Can the Military Benefit from Corporate use of Strategic Information Systems Planning?* Monterey: Naval Postgraduate School, 1999.

Network Centric Warfare: Report to Congress, Department of Defense. *Network Centric Warfare: Report to Congress.* Washington, D.C.: Department of Defense, 2001.

Newkirk, Henry E, Albert L Lederer, and Alice M Johnson. "Rapid business and IT change: drivers for strategic information systems planning?" *European Journal of Information Systems*, 2008: 198-218.

Newkirk, Henry E, Albert L Lederer, and Cidambi Srinivasan. "Strategic information systems planning: too little or too much?" *Journal of Strategic Information Systems*, 2003: 201-228.

Newkirk, Henry E, and Albert L Lederer. "The Effectivness of Strategic Information Systems Planning for Technical Resources, Personnel Resources, and Data Security in Evironments of Heterogeneity and Hostility." *Journal of Computer Information Systems*, 2007: 34-44.

Newkirk, Henry E, and Albert L Lederer. "The Effectivness of strategic information systems planning under environmental uncertainty." *Information & Management*, 2006: 481-501.

Nunnally, Jum C. *Psychometric Theroy.* Second Edition. McGraw-Hill, 1978.

Occupational Information Network. *11-1011.00 - Chief Executives.* May 5, 2010. http://online.onetcenter.org/link/summary/11-1011.00 (accessed May 5, 2010).

Office of Public Affairs, Department of Defense. "2010 QDR Terms of Reference Fact Sheet." 2009.

Papp, Raymond, and Jeff Lackey. "Strategic Alignment: Analysis of Perspectives." *Tampa Bay Technology Leadership Association.* 2007. www.tb-tla.org/docs/TBTLA051007.ppt (accessed May 31, 2010).

Peppard, Joe, and John Ward. "Beyond strategic information systems: towards an IS capability." *Journal of Strategic Information Systems*, 2004: 167-194.

Philip, George. "IS Strategic Planning for Operational Efficiency." *Information Systems Management*, 2007: 247-264.

Pollalis, Yannis A. "Patterns of co-alignment in information-intensive organizations: business performance through integration strategies." *International Journal of Information Management*, 2003: 469-492.

Powell, Philip. "Causality in the Alignment of Information Technology and Business Strategy." *Journal of Strategic Information Systems*, 1993: 320-334.

Premkumar, G, and William R King. "Assessing Strategic Information Systems Planning." *Long Range Planning*, 1991: 41-58.

Public Law No. 96-511. *Paperwork Reduction Act (44 U.S.C. 3501 et seq.).* Washington, DC.: Congress, 1980.

Public Law No.104-106, Division E. *Clinger-Cohen Act.* Wahington, DC.: Congress, 1996.

Pulvermacher, Mary K. *Implementing a Net-Centric Data Access Service.* MITRE Corporation, 2008.

Raghunathan, B, and T S Raghunathan. "Adaptation of a Planning System Success Model to Information Systems Planning." *Information Systems Research*, 1994: 326-340.

Reich, Blaize H, and Izak Banbasat. "Measuring the Linkage Between Business and Information Technology Objectives." *MIS Quarterly*, 1996: 55-81.

Reich, Blaize H, and Izak Benbasat. "Factors that Influence the Social Dimension of Alignment between Business and Information Technology Objectives." *MIS Quarterly*, 2000: 81-113.

Ryan, Julie J.C.H., and Theresa I Jefferson. "The Use, Misuse, and Abuse of Statistics in Information Security Research." *Proceedings of the 2003 ASEM National Conference.* St. Louis, MO, 2003.

Sabherwal, Rajiv, and Yolande E Chan. "Alignment Between Business and IS Strategies: A Study of Prospectors, Analyzers, and Defenders." *Information Systems Research*, 2001: 11-33.

Schudel, Gregg, and Bradley Wood. "Adversary Work Factor as a Metric for Information Assurance." *Association for Computing Machinery*, 2001.

Segars, Albert H, and Varun Grover. "Strategic Information Systems Planning Success: An Investigation of the Constructs and Its Measurement." *MIS Quaterly,* 1998: 139-163.

Segars, Albert H, Varun Grover, and T C Teng. "Strategic Information Systems Planning: Planning System Dimensions, Internal Coalignment, and Implications for Planning Effectivness." *Decision Sciences*, 1998: 303-345.

Sen, Dhruba. "Using IT to Support Business Strategy." *Accountancy*, 2007: 137-140.

Statistics Solutions. *Kruskal-Wallis Test.* 2009. http://www.statisticssolutions.com/methods-chapter/statistical-tests/kruskal-wallis-test/ (accessed March 2010).

Stenbit, John P. "Horizontal Fusion: Net-Centric Operations and Warfare." *The Journal of Defense Software Engineering*, 2004: 4.

Strassmann, Paul A. *Does the 2009 Budget Support Network-Centric Missions?* November 2008. http://www.afcea.org/signal/articles/anmviewer.asp?a=1748&print=yes (accessed October 17, 2009).

Tampa, The University of. *Tampa Bay Technology Leadership Association.* June 7, 2010. http://www.tb-tla.org/index.htm (accessed June 7, 2010).

Teo, Thompson S. H., and William R King. "Integration between Business Planning and Information Systems Planning: An Evolutionary-Contingency Perspective." *Journal of Management Information Systems*, 1997: 185-214.

Teunber, R A. "Strategic information systems planning: A case study from the financial services industry." *Journal of Strategic Information Systems*, 2007: 105-125.

Trochim, William K, and James P Donnelly. *The Research Methods Knowledge Base.* Mason, OH: Atomic Dog, 2008.

United States Government Accountablity Office. *Defense Acquisitions: The Golbal Information Grid and Challenges Facing Its Implementation (GAO-04-858).* Washington, D.C.: GAO, 2004.

Venkatraman, N, and Vasudevan Ramanujam. "Planning System Success: A Conceptualization and an Operational Model." *Management Sciences*, 1987: 687-705.

Williams, Deryck. "Are you IT-dependent?" *CA Magazine*, August 2002: 30-32.

Yarberry, William A. "Effective Change Management: Ensuring Alignment of IT and Business Funations." *Change Management*, 2005: 12-24.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
05-17-2010	Master's Thesis	May 2008 – June 2010

4. TITLE AND SUBTITLE
Assessing the Alignment of Information Security with Strategic Business, and Strategic Information System Planning: A Department of Defense perspective.

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Scanlan IV, John H

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/10-J02

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Intentionally left blank

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This research extends the Strategic Information Systems Plan (SISP) and Strategic Business Plan (SBP) alignment model construct by adding the Information Security Plan (ISP) as an additional component considered essential to the success of network centric organizations. Six hypotheses were considered to measure the two-way alignment among three components of the proposed model. The research was adapted for a public sector organization and analyzed using the Kruskal-Wallis non-parametric test. A vertical, cross-sectional sample from the United States Marine Corps, a Department of Defense organization, was surveyed (n = 149). Results indicate a strong two-way alignment exists between SISP - SBP (p = .232 and .910), between SISP - ISP (p = .445 and .467), and between SBP - ISP (p = .205 and .490). The research instrument developed in this work enables the evaluation of public and private sector organizations determine the strength of their strategic alignment in terms of security, information technology, and business objectives.

15. SUBJECT TERMS

Strategic Alignment, Network Centric Organizations, Strategic Business Planning, Strategic Information Systems Planning.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Dr. Michael R. Grimaila
U	**U**	**U**	**UU**	145	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 4800 (michael.grimaila@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18